Schriften zum Öffentlichen Recht

Band 1426

Der Grundsatz digitaler Souveränität

Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung

Von

Christian Ernst

Duncker & Humblot · Berlin

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

CHRISTIAN ERNST

Der Grundsatz digitaler Souveränität

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Schriften zum Öffentlichen Recht

Band 1426

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Der Grundsatz digitaler Souveränität

Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung

Von

Christian Ernst

Duncker & Humblot · Berlin

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Alle Rechte vorbehalten
© 2020 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpar
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-15931-4 (Print)
ISBN 978-3-428-55931-2 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Geleitwort

Können Sie sich noch an die in den achtziger Jahren geplante Volkszählung erinnern? Mit Befragern an der Haustür sollten vor allem Haushaltsgrößen ermittelt werden. Massive Proteste behinderten damals die Durchführung. Man fürchtete, zum „gläsernen Menschen“ zu werden. Heute liefert schon das Einschalten Ihres Smartphones ein Vielfaches der Daten aus, die damals so vehement verweigert wurden. Es scheint, als habe die Digitalisierung in kürzester Zeit zu einer vollkommen anderen Wahrnehmung von Sicherheitserfordernissen und Persönlichkeitsschutzrechten geführt. Die Menschen gehen mit ihren Daten und mit Daten über sie vor allem dann einigermaßen bedenkenlos um, wenn sie es mit Geräten, Apps und Leistungen privater Anbieter zu tun haben. Google, Facebook, Amazon und Apple werden permanent ungeheure Datenmengen geschenkt. Daten, die Spiegel unserer Selbst sind, die uns mitunter besser und treffender beschreiben als dies gute Freunde tun könnten. Die uns vor allem auch wortwörtlich berechenbar machen.

Man mag diesen geradezu freiwilligen Verlust digitaler Souveränität im privaten Bereich bedauern. Mit Blick auf Daten, die vom Staat verarbeitet werden, ist er inakzeptabel. Man stelle sich vor, Meldedaten oder Daten der Finanzverwaltung würden über US-amerikanische Server von Unternehmen laufen, die daraus Erkenntnisse zur Maximierung ihres Geschäftserfolgs gewinnen würden. Was hier spontan abwegig erscheint, ist jedoch mithin möglich. Denn die technisch notwendigen Fähigkeiten zur Entwicklung und Beherrschung einer IT mit den hohen Anforderungen an Sicherheit und Verfügbarkeit, wie sie an staatliche Datenverarbeitung geknüpft sind, übersteigen die Möglichkeiten einzelner staatlichen Stellen. Es wäre auch, wie es im nachfolgenden Gutachten heißt, „in höchstem Maße ineffizient, würde jede einzelne zuständige Stelle selbst vollumfänglich ausreichende technische Fähigkeiten für die notwendige Datenverarbeitung vorhalten“ (15).

Als Alternative bietet sich somit die Beschaffung externer Kapazitäten an (15). Es liegt jedoch in ihrer technischen Natur, dass Daten „schlüpfrig“ sind: Sie sind schnell, ohne nennenswerten Aufwand und mit geringen Kosten zu übertragen – und mit jeder Übertragung und jeder Zugriffsmöglichkeit wächst die Gefahr, dass Daten den Weg in die Öffentlichkeit finden. Und während Kontrolle bei anderen Aufgabenprivatisierungen zumindest im Nachhinein wiederherstellbar ist, können die Folgen von Datenverlust oder -missbrauch häufig nicht mehr rückgängig gemacht werden (40). Die nachträgliche Missbrauchskontrolle, die sonst üblich ist, greift bei Daten nicht (76).

Und werden staatliche Daten an einen privaten IT-Dienstleister übermittelt, sind zumindest außerbehördliche Zugriffsmöglichkeiten möglich. Keine Frage, dass dies

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

besondere Vorkehrungen erforderlich macht. Die Verantwortlichkeiten müssen dabei klar geregelt sein und verbindlich vereinbart werden. Das vorliegende Gutachten beschreibt ausführlich, welche Kriterien und Maßstäbe dabei anzulegen sind, welche Risiken mithin dabei „eingekauft" werden.

Der Wunsch nach Erhalt der digitalen Souveränität durch staatliche Akteure besteht im wahrsten Sinne des Wortes zu Recht: Denn digitale Souveränität ist ein Rechtsprinzip – verfassungsrechtlich und einfachgesetzlich gegründet. Der Staat hat, anders als die gewinnorientierten Datensammler der Internetökonomie, kein geschäftliches Interesse an den Daten der Bürgerinnen und Bürger. Die Behörden arbeiten mit diesen Daten, um zum Beispiel Aufgaben der Steuerverwaltung, des Meldewesens oder der Arbeits- und Sozialverwaltung zu erledigen. Damit die Informationsmacht des Staates begrenzt ist, bestimmt allein die Aufgabenerfüllung den Zweck der Datenverarbeitung: Staatsfinanzierung, Sicherheit, Ordnung, Fürsorge. Die Grundwerte unserer Verfassung, Menschenwürde, Gleichberechtigung, soziale Teilhabe, demokratische Mitgestaltung, Rechtsstaatlichkeit und Beteiligung der Sozialpartner müssen die Richtschnur bei der Entwicklung digitaler Geschäftsprozesse der staatlichen Verwaltung sein.

Denn es ist die Aufgabe des Staates, die digitale Souveränität der Bürgerinnen und Bürger zu schützen und zu gewährleisten. Und seine eigene digitale Souveränität – denn auch diese ist gefährdet, wenn Algorithmen, Analysetechnologie und Infrastruktur überwiegend oder gar allein in den Händen großer Technologiekonzerne liegen, die mitunter weder europäischen Rechtsnormen unterliegen noch unseren ethischen Maßstäben verpflichtet sind.

So stellt sich den Trägern öffentlicher Gewalt also die Frage, welcher Weg der Staat zur Aufrechterhaltung und Entwicklung einer leistungs- und zukunftsfähigen Informationstechnik beschreiten sollte und beschreiten kann. Denn neben rein privaten IT-Dienstleistern gibt es auf der Ebene des Bundes, der Länder und Kommunen viele IT-Dienstleister, die von der öffentlichen Hand getragen werden. In einzelnen Sachbereichen herrscht hierzu eine einfachgesetzliche Rechtslage, etwa die §§ 17 Abs. 3,2 Abs. 2 FVG für die Finanzverwaltung oder für die digitale Führung des Grundbuchs entsprechend § 126 Abs. 3 GBO (15). Abseits solcher Einzelfallregelungen fehlt es jedoch an generellen Vorgaben. Dabei bedarf das Ringen nach digitaler Souveränität gerade jetzt, auf dem unumkehrbaren Weg in die Digitalisierung der Verwaltung, solch allgemeingültiger Direktiven. Staatliche Souveränität – und damit auch die digitale Souveränität des Staates – hat Verfassungsrang. Jedoch stellen die materiellen Verfassungsnormen im Hinblick auf die Teilung von Aufgaben zwischen staatlichen und privaten Dienstleistern nicht mehr als eine Rahmenordnung bereit. Somit bleiben unterschiedlichste Konstellationen und Formen der Verarbeitung von Daten der Bürgerinnen und Bürger möglich. Bis hin zu solchen, die daran zweifeln lassen, ob der Staat noch ein von ihm gesteuertes und damit auch rechtlich gebundenes digitales Verwaltungshandeln gewährleisten kann. Nicht umsonst wird der Ruf lauter nach einer Harmonisierung der verwaltungsrechtlichen

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Digitalnormen, die über eine Vielzahl von Einzelgesetzen (VwVfG, eGovG, OZG, DSGVO, Fachgesetze etc.) verstreut sind.

Als Anstoß zu einer dringend erforderlichen Diskussion dahingehend haben wir das nachfolgend veröffentlichte Gutachten in Auftrag gegeben. Die zentrale Fragestellung der wissenschaftlichen Ausarbeitung ist: „Wie kann die digitale Souveränität des Staates selbst im Kontext der zunehmenden Digitalisierung sichergestellt werden?"

Das Gutachten zeigt eindrucksvoll das Spannungsfeld, in dem sich die staatliche Informationsverarbeitung bewegt: Einerseits ist der Schutzauftrag des Staates in Deutschland hinsichtlich der digitalen Souveränität seiner Bürgerinnen und Bürger verfassungsrechtlich gegründet in den objektiv-rechtlichen Schutzgehalten diverser Grundrechte sowie des Staatsauftrags. Auf der anderen Seite braucht es jedoch ein begründetes Vertrauen der Bürgerinnen und Bürger in die digitale Selbstbestimmung und Handlungsfreiheit des Staates selbst – sowie darin, dass persönliche Daten ausschließlich im Rahmen der Zweckbindung genutzt werden. Eine entsprechende Gewährleistungsverantwortung des Staates muss die Gemeinwohlverträglichkeit einer Aufgabenerfüllung durch private Akteure sicherstellen – was gerade bei der Datenverarbeitung mit besonderen Schwierigkeiten verbunden ist.

Ohne Vertrauen gibt es keine Akzeptanz der Online-Verwaltung. Mehr noch: Der Autor formuliert, dass „ein allgemeines Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen als zwingende Voraussetzung für den demokratischen Rechtsstaat angesehen werden" kann (68). Dass aber auch ein besonderes Maß an Vertrauen gerade in solchen Bereichen notwendig ist, „die sich neu entwickeln, für den Einzelnen unbekannt sind und für die Erfahrungen fehlen" (67) – also gerade im Zuge des aktuell stattfindenden Umbruchs von herkömmlichen zu digitalen Prozessen, der Digitalisierung.

Und gerade dieses Vertrauen geht schnell verloren. Während man auch schon beinahe verniedlichend von „Datenpanne" spricht, wenn Facebook millionenfach persönliche Daten „verliert", würden Fehler in weitaus geringerem Maße im Zusammenhang mit staatlicher IT den Glauben an die Gemeinwohlverpflichtung der Verwaltung insgesamt erschüttern.

Der Autor des Gutachtens stellt fest: „Es fehlen generelle und allgemeingültige Vorgaben, in welchen Konstellationen Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen dürfen" (16). Sie sehen insbesondere unter dem Aspekt eines drohenden Vertrauensverlustes in die Integrität und Leistungsfähigkeit staatlicher IT, dass ein vertrauensvoller Umgang mit Daten nur dann möglich ist, „wenn von vornherein und eindeutig klar ist, dass diese in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben, der durch unmittelbare Grundrechts- und Gesetzesbindung gekennzeichnet ist" (76).

Ich freue mich sehr, Ihnen mit dem nachstehenden Gutachten eine wissenschaftliche Sicht auf den Sachkomplex zu präsentieren, die in einer beherzt geführten

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Diskussion für mehr Klarheit sorgt. Sie verschafft Ihnen damit mehr Entscheidungssicherheit bei einer Aufgabe, die eine der wohl weitreichendsten staatlichen Aufgaben des 21. Jahrhunderts ist – die Wahrung unserer digitalen Souveränität.

Hamburg/Altenholz, im Oktober 2019 *Dr. Johann Bizer*
Vorstandsvorsitzender Dataport

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Vorwort

Das vorliegende Gutachten habe ich im Auftrag von Dataport AöR erstellt. Ausgangspunkt war der Eindruck, dass die Frage, wann und in welchem Ausmaß sich Träger öffentlicher Gewalt bei der Wahrnehmung ihrer Aufgaben privater IT-Dienstleister bedienen dürfen, in der Rechtswissenschaft kaum geklärt ist, insbesondere im Hinblick auf grundsätzliche Strukturen, die diesem Bereich zugrunde liegen. Dabei liegt es auf der Hand, dass dieser Frage im Zuge der fortschreitenden Digitalisierung der öffentlichen Verwaltung eine erhebliche Relevanz zukommt. Denn mit der zunehmenden Bedeutung von Informationstechnologien können auch die Unternehmen, die über diese Technologien verfügen und sie der öffentlichen Hand zur Verfügung stellen, einen stetig wachsenden Einfluss auf die Ausübung staatlicher Befugnisse erhalten.

Dass es sich hierbei nicht nur um theoretische Überlegungen handelt, zeigt sich immer deutlicher. So war unlängst zu erfahren, dass die Bundespolizei die Aufnahmen ihrer Bodycams in einer Amazon-Cloud speichert. Das Unternehmen ist nicht nur der prägende Akteur im Online-Einzelhandel, sondern als Amazon Web Services auch führender internationaler Anbieter von Cloud Computing. Und im Rahmen des Ausbaus des 5G-Netzes diskutieren Fachkreise öffentlich, ob die Mitwirkung des chinesischen Netzwerkausrüsters Huawei ein Sicherheitsproblem darstellt. Angesichts dieser Entwicklung liegt die Frage, ob private Unternehmen einen unverhältnismäßig großen und möglicherweise gefahrbringenden Einfluss auf die Funktionsfähigkeit der Verwaltung oder grundlegender Infrastrukturen bekommen, nahe.

Herrn Johannes Franke danke ich für wertvolle Unterstützung und Diskussionen. Frau Pauline Rachor danke ich für Hilfe bei der Erstellung des Manuskripts.

Hamburg, Oktober 2019 *Christian Ernst*

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Inhaltsverzeichnis

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

A. Einleitung

Für Träger staatlicher Gewalt ist die Verwendung von Daten untrennbar mit der alltäglichen Aufgabenwahrnehmung verbunden. Dabei übersteigen die technisch notwendigen Fähigkeiten immer öfter die Möglichkeiten einzelner staatlicher Stellen, die für die spezifische Aufgabenwahrnehmung zuständig sind. Für die Staatsgewalt wäre es – ebenso wie für viele Private – in höchstem Maße ineffizient, würde jede einzelne zuständige Stelle selbst vollumfänglich ausreichende technische Fähigkeiten für die notwendige Datenverarbeitung vorhalten.

Als Alternative bietet sich die Beschaffung externer Kapazitäten an. Werden staatliche Daten an einen privaten IT-Dienstleister übermittelt, können sich dadurch aber tatsächliche Zugriffsmöglichkeiten des Privaten auf die staatlichen Daten ergeben. Dies kann besondere Vorkehrungen erforderlich machen. Zugleich existiert mittlerweile auf den Ebenen des Bundes, der Länder und der Kommunen sowie anknüpfend an einzelne Sach- und Geschäftsbereiche eine Vielzahl öffentlicher IT-Dienstleister. Im Hinblick auf solche Formen des IT-Outsourcing[1] stellt sich Trägern öffentlicher Gewalt deshalb stets die Frage, ob sie IT-Dienstleister, die von der öffentlichen Hand getragen werden, oder private IT-Dienstleister in Anspruch nehmen.

Die Praxis zeichnet ein differenziertes Bild. Teilweise scheint die öffentliche Gewalt keine gesteigerten Berührungsängste vor privaten IT-Dienstleistern zu haben. Ein Beispiel bildet die Zusammenarbeit der Bundespolizei mit Amazon Web Services bei der Speicherung der Aufnahmen von Bodycams.[2] In anderen Fällen hingegen werden Vorbehalte gegen die Einbindung privater IT-Unternehmen auch in der Öffentlichkeit breit diskutiert, etwa solche gegen die Einbeziehung des chinesischen Netzwerkausrüsters Huawei beim Aufbau des 5G-Netzes.

Die Rechtsordnung gibt auf die Frage, ob ein Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen darf, lediglich für einzelne Sachbereiche eine ausdrückliche Antwort.[3] Für die Finanzverwaltung etwa bestimmen die §§ 17 Abs. 3, 2 Abs. 2 FVG, dass nur Rechenzentren der Landesfinanzverwaltung mit Datenverarbeitungsaufgaben betraut werden dürfen und für die digitale Führung des Grundbuchs erlaubt § 126 Abs. 3 GBO unter bestimmten Umständen eine externe Datenverarbeitung (lediglich) auf den Anlagen einer anderen staatlichen Stelle oder

[1] Zum Begriff des IT-Outsourcing *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 1 ff.; *Ulmer*, CR 2003, 701 (702). Vgl. auch *Zundel*, CR 1996, 763.

[2] BT-Drs. 19/8180, S. 15, 22.

[3] Vgl. auch Nr. 2 des Beschluss Nr. 2015/5 des Rates der IT-Beauftragten der Ressorts vom 29. 7. 2015.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

auf den Anlagen einer juristischen Person des öffentlichen Rechts. § 30 Abs. 9 AO lässt mittlerweile eine Auftragsverarbeitung i.S.d. DSGVO nur dann zu, wenn die Daten ausschließlich durch Personen verarbeitet werden, die zur Wahrung des Steuergeheimnisses verpflichtet sind. Nach § 30 Abs. 1 AO sind damit grundsätzlich Amtsträger angesprochen und § 30 Abs. 3 AO erweitert dies auf die für den öffentlichen Dienst besonders verpflichteten Personen (vgl. § 11 Abs. 1 Nr. 4 StGB).

Abseits solcher Einzelfallregelungen werden die Voraussetzungen und Schranken einer Inanspruchnahme privater IT-Dienstleister durch Träger staatlicher Gewalt bislang kaum diskutiert und problematisiert.[4] Es fehlen generelle und allgemeingültige Vorgaben, in welchen Konstellationen Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen dürfen. Den dahinterstehenden Fragen soll die vorliegende Untersuchung nachgehen.

Bei diesem Vorgehen wird ein Grundsatz digitaler Souveränität deutlich werden, der zur Konsequenz haben kann, dass Daten ausschließlich in einer öffentlich-rechtlich geprägten Herrschaftssphäre verbleiben müssen und nicht Privaten übertragen werden dürfen. Bestehende einfachgesetzliche Regelungen, die in diese Richtung zielen, lassen sich als Konkretisierung dieses Grundsatzes verstehen.

[4] Ebenso *Heckmann*, in: ders. (Hrsg.), jurisPK-Internetrecht, Kap. 5 Rn. 164; *ders./Braun*, BayVBl. 2009, 581 (581); vgl. *Petri/Dorfner*, ZD 2011, 122 (127). Vgl. zu den konkreten Modalitäten einer Privatisierung *Schubert*, Privatisierung des eGovernments, S. 201 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

B. Untersuchungsgegenstand

Der Grundsatz digitaler Souveränität soll hier nicht im Sinne einer staatlichen Kontrolle über die Funktionsweise von staatlich eingesetzter Hard- oder Software verstanden werden. Stattdessen geht es um die Frage, ob es für Träger staatlicher Gewalt zulässig ist, Daten aus ihrem alleinigen, öffentlich-rechtlich geprägten Einflussbereich zu entlassen und stattdessen einem Privaten einen zumindest mittelbaren Zugriff auf die Daten – etwa durch die tatsächliche Verfügungsgewalt über den physischen Datenträger – zu ermöglichen.

Relevant werden kann dies etwa bei der Nutzung privater Cloud-Dienste oder privater Rechenzentren durch Träger staatlicher Gewalt. Denn damit kann die Übertragung einer eigenständigen Verfügungsmacht auf Private einhergehen, die unabhängig vom Willen Dritter ausgeübt werden kann, auch wenn sich diese lediglich mittelbar über den tatsächlichen Zugriff auf die physischen Datenträger ergibt. Angesprochen ist damit eine Art materielle Privatisierung der (zumindest tatsächlichen) Verfügungsbefugnis über Daten. Grundsätzlich nicht erreicht werden dürfte dieser Zustand bei privaten Unterstützungsleistungen wie IT-Wartungsarbeiten.

Falls es zu einer Übermittlung staatlicher Daten in private Herrschaftssphären kommt, wird hierfür nach datenschutzrechtlichem Verständnis in aller Regel ein Auftragsverarbeitungsverhältnis in Betracht kommen. Die vorliegende Untersuchung bezieht sich indes allein mittelbar auf Auftragsverarbeitungsverhältnisse und konzentriert sich stattdessen auf die grundlegendere Schwelle zwischen einem hoheitlich und einem privat geprägten Einflussbereich und die damit zusammenhängenden (tatsächlichen) Einwirkungsmöglichkeiten bzw. Einwirkungsgrenzen auf die fraglichen Daten.[1] Eine sog. Funktionsübertragung auf Private nach datenschutzrechtlichem Verständnis, bei der sogar selbständige Entscheidungsbefugnisse eingeräumt werden,[2] ist dafür eine hinreichende, aber keine notwendige Bedingung und soll deshalb hier nicht der entscheidende Maßstab sein. Über diese allgemeine Gegenüberstellung von hoheitlich und privat geprägten Einflussbereichen hinaus sollen die zusätzlichen Voraussetzungen, die sich in internationalen und grenzüberschreitenden Konstellationen ergeben können, nicht näher betrachtet werden.

[1] Zu solchen Machtbereichen vgl. *Griesser/Buntschu*, DuD 2016, 640 (645).

[2] Vgl. zur Funktionsübertragung bei der Datenverarbeitung und der Frage, inwiefern diese unter der DSGVO eigenständige Bedeutung hat, *Spoerr*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 28 DSGVO Rn. 23 ff.; *Ingold*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 28 Rn. 15 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Ein hoheitlich geprägter Einflussbereich ist in erster Linie dann gewahrt, wenn Daten unmittelbar durch die Behörden und Organe einer juristischen Person des öffentlichen Rechts selbst verarbeitet werden. Bei der Einbeziehung von IT-Dienstleistern kann der hoheitlich geprägte Einflussbereich auch zumindest dann angenommen werden, wenn der einbezogene IT-Dienstleister eine Rechtsform des öffentlichen Rechts aufweist und daher grundrechtsgebunden sowie dem Gesetzesvorbehalt und -vorrang unterworfen ist. Typischerweise kommt hierfür das Konstrukt der Anstalt des öffentlichen Rechts in Betracht, wie z. B. im Falle von Dataport, dem IT-Dienstleister für die Landesverwaltungen von Hamburg, Bremen, Schleswig-Holstein und Sachsen-Anhalt, für die Steuerverwaltungen von Mecklenburg-Vorpommern und Niedersachsen sowie für schleswig-holsteinische Kommunen, oder der ITEOS, die baden-württembergische Kommunen bei der IT-Dienstleistung unterstützt. Daneben existieren öffentliche IT-Dienstleister, die keine eigene Rechtspersönlichkeit aufweisen, sondern etwa als Behörde dem Geschäftsbereich eines bestimmten Ministeriums zugeordnet sind. Ein Beispiel bildet noch das Informationstechnikzentrum Bund (ITZBund), derzeit eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums der Finanzen. Für das ITZBund ist jedoch im aktuellen Koalitionsvertrag festgehalten, dass es in eine Anstalt des öffentlichen Rechts umgewandelt werden soll.[3] Auf Landesebene sind als Landesbetrieb z. B. die Hessische Zentrale für Datenverarbeitung (HZD) im Geschäftsbereich des Hessischen Ministers der Finanzen[4] oder der Landesbetrieb Daten und Information (LDI) in Rheinland-Pfalz organisiert.

Dem staatlichen Bereich können auch noch – zumindest begrifflich – IT-Dienstleister zugeordnet werden, die zwar in einer privaten Rechtsform betrieben, aber vollständig von einem Träger öffentlicher Gewalt gehalten werden, wie z. B. der BWI GmbH als zentralem IT-Dienstleister der Bundeswehr, die zu 100 % vom Bund getragen wird, oder der DVZ M-V GmbH, deren alleiniger Gesellschafter das Land Mecklenburg-Vorpommern ist. Die Frage, inwieweit in diesen Fällen noch von einem öffentlich-rechtlich geprägten Einflussbereich gesprochen werden kann, soll hier zwar nicht vertieft werden. Es wird sich aber zumindest zeigen, dass, je stärker die Rechts- und Handlungsformen eines IT-Dienstleisters privatrechtlich ausgestaltet sind, desto schneller Grenzen für deren Einbindung in die Wahrnehmung staatlicher Aufgaben erreicht sein können. Schließlich erscheinen auch gemischtwirtschaftliche Unternehmen in diesem Bereich denkbar.

Diese Abhandlung zielt nicht darauf ab, das Handeln einzelner (privater oder öffentlicher) IT-Dienstleister oder konkrete Gestaltungen von Vertragsbeziehungen zum Gegenstand zu machen. Vielmehr sollen die abstrakten Grundlagen einer Einbindung privater IT-Dienstleister in die Wahrnehmung staatlicher Aufgaben

[3] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, S. 46. Der Beschluss des IT-Rat vom 19. 9. 2016, Nr. 2016/9, spricht sogar davon, dass die Änderung der Rechtsform im Laufe des Jahres 2019 erfolgen sollte.

[4] Beschluss über die Zuständigkeiten der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 4. 4. 2019.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

näher ergründet werden. Zu diesem Zweck soll untersucht werden, inwiefern die abstrakten normativen Rahmenbedingungen für Private und Träger öffentlicher Gewalt unterschiedliche Verhaltensstandards begründen können.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

C. Grundsatz digitaler Souveränität

Der Grundsatz digitaler Souveränität kann sich zur Begründung auf drei Säulen stützen: obligatorische Staatsaufgaben, eine staatliche Gewährleistungsverantwortung und das Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien. Diese drei Begründungsansätze vermögen im Einzelfall schon für sich betrachtet den Grundsatz digitaler Souveränität und die Notwendigkeit zu rechtfertigen, dass staatliche Daten allein in einer öffentlich-rechtlich geprägten Herrschaftssphäre verbleiben dürfen. Häufig werden sich in konkreten Anwendungsfällen die drei Begründungssäulen aber überschneiden und nebeneinander ihre Wirkung entfalten. Veranschaulicht werden soll dies im Laufe der Untersuchung jeweils mit einfachgesetzlichen Beispielen, die sich als Ausdruck des Grundsatzes digitaler Souveränität deuten lassen.

I. Vorüberlegung

Die Frage nach der Zulässigkeit einer Auslagerung staatlicher Daten auf Private verweist auf die allgemeine Diskussion um Staatsaufgaben und die (verfassungsrechtlichen) Grenzen der Privatisierung.[1] Dieses Thema hatte zuletzt vor dem Hintergrund der Privatisierungs- und Liberalisierungswelle verstärkte Aufmerksamkeit erfahren, welche gegen Ende des vergangenen Jahrhunderts insbesondere den Bereich der Daseinsvorsorge erfasste. Im Ergebnis besteht weitestgehend Einigkeit, dass sich der Verfassung grundsätzlich kaum konkrete oder gar abschließende Aussagen über die allgemeine Aufgabenverteilung zwischen Staat und Gesellschaft entnehmen lassen.[2]

1. Kein ausdrücklicher Kanon an obligatorischen Staatsaufgaben

Das Grundgesetz enthält keinen bestimmten oder gar abschließenden Katalog an Staatsaufgaben. Die Kompetenzbestimmungen des Grundgesetzes betreffen primär den staatlichen Binnenbereich und treffen keine konkreten Aussagen zur Aufga-

[1] Vgl. aus der Fülle der Literatur nur *Bull*, Die Staatsaufgaben nach dem Grundgesetz; *Kämmerer*, Privatisierung; *Weiß*, Privatisierung und Staatsaufgaben.

[2] Statt vieler *Voßkuhle*, VVDStRL 62 (2003), 266 (274 f.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

benverteilung zwischen Staat und Gesellschaft.[3] Im Bereich der obligatorischen Bundesverwaltung (vgl. Art. 87 Abs. 1 S. 1, 87b, 87d GG) lässt sich der Verfassung zumindest entnehmen, dass jedenfalls der Kern der genannten Aufgabenbereiche einer Privatisierung verschlossen ist.[4] Ähnliches soll nach der Rechtsprechung für zentrale Aufgaben der gemeindlichen Selbstverwaltung (Art. 28 Abs. 2 GG) gelten, wobei die Grenzen unklar und umstritten sind.[5] Der Beamtenvorbehalt in Art. 33 Abs. 4 GG setzt nach herrschender Meinung eine staatliche Aufgabenwahrnehmung voraus und ordnet sie nicht an;[6] abermals soll die Norm allenfalls einen minimalen Kernbestand staatlicher Aufgaben garantieren.[7] Die materiellen Verfassungsnormen – Grundrechte sowie Staatszielbestimmungen und -strukturprinzipien – sind wiederum in hohem Maße interpretations- und abwägungsbedürftig. Im Hinblick auf die Aufgabenverteilung zwischen staatlichen und privaten Akteuren stellen sie nicht mehr als eine Rahmenordnung[8] bereit, die grundsätzlich Raum für ganz unterschiedliche Konstellationen und Kooperationen lässt.[9]

Angesichts dieses Befundes hat sich in der verfassungsgerichtlichen Rechtsprechung und der Staatsrechtslehre weitgehend der sog. formale Staatsaufgabenbegriff durchgesetzt, wonach Staatsaufgaben schlicht diejenigen Aufgaben sind, mit denen sich der Staat mittels seiner Organisationseinheiten in irgendeiner Form befasst.[10] In diesem Sinne kann auch die Verarbeitung behördlich erhobener Daten eine Staatsaufgabe sein, ohne dass damit irgendeine Aussage über die Zulässigkeit einer Einbindung Privater verbunden wäre.

---

[3] *März*, in: v. Mangoldt/Klein/Starck, GG, Art. 30 Rn. 39 ff.; vgl. auch *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 152 ff.

[4] *Sachs*, in: ders. (Hrsg.), GG, Art. 87 Rn. 23 f.; *Burgi*, in: v. Mangoldt/Klein/Starck, GG, Art. 87 Abs. 1 Rn. 28; ferner *Kokott*, in: Sachs (Hrsg.), GG, Art. 87b Rn. 2; *Windthorst*, in: Sachs (Hrsg.), GG, Art. 87d Rn. 8.

[5] BVerwG NVwZ 2009, 1305; *Dreier*, in: ders. (Hrsg.), GG, Art. 28 Rn. 125 m.w.N.

[6] *Jachmann-Michel/Kaiser*, in: v. Mangoldt/Klein/Starck, GG, Art. 33 Abs. 4 Rn. 38; *Thiele*, Der Staat 49 (2010), 274 (288).

[7] Zur Diskussion näher *Brosius-Gersdorf*, in: Dreier (Hrsg.), GG, Art. 33 Rn. 151 ff. m.w.N. Zu den staatlichen „Kernaufgaben" noch näher unten C. II. 1.

[8] Zur Charakterisierung der Verfassung als Rahmenordnung grundlegend *Böckenförde*, NJW 1976, 2088 (2091); mit Blick auf Privatisierungsprozesse *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 13: „Privatisierungs-Rahmenordnung".

[9] Statt vieler *Voßkuhle*, VVDStRL 62 (2003), 266 (275 ff.); *Schuppert*, Staatswissenschaft, S. 292 ff.

[10] BVerfGE 12, 205 (243); *Burgi*, Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, Gutachten für den 67. DJT, S. 14 f.; *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 13.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

2. Keine Pflicht zur Privatisierung

Aus dem bloßen Rahmencharakter der Verfassung folgt umgekehrt, dass sich aus dem Grundgesetz keine grundsätzlichen Rechtspflichten zur Privatisierung ableiten lassen.[11] Eine staatliche Aufgabenwahrnehmung ist keineswegs allgemein „subsidiär" gegenüber einer Wahrnehmung durch gesellschaftliche Kräfte bzw. den Markt[12] und greift in aller Regel nicht in die Grundrechte potenziell konkurrierender privater Unternehmen ein. Die Berufsfreiheit (Art. 12 Abs. 1 GG) gewährt nach der Rechtsprechung des Bundesverwaltungsgerichts keinen Schutz vor staatlicher Konkurrenz, „solange die private wirtschaftliche Betätigung nicht unmöglich gemacht oder unzumutbar eingeschränkt wird oder eine unerlaubte Monopolstellung entsteht".[13]

Eine solche Monopolisierung ist aber nicht etwa schon darin zu sehen, dass der Staat bestimmte Leistungen „an sich selbst" erbringt, statt sie am Markt einzukaufen. Grundrechtlich problematisch wird es erst dann, wenn ein gesamter Tätigkeitsbereich dem Staat vorbehalten wird.[14] Daher ist es verfassungsrechtlich unproblematisch, wenn staatliche Stellen im Bereich der Datenverarbeitung Aufgaben wahrnehmen, die auch von der Privatwirtschaft angeboten werden.[15] Es gibt keinen grundrechtlichen Anspruch darauf, dass die öffentliche Hand die in ihrem Aufgabenkreis anfallenden Tätigkeiten auch für Private öffnet und diesen überträgt.[16] Grundrechte Privater werden durch Regelungen, die eine Verarbeitung behördlich erhobener Daten ausschließlich (anderen) behördlichen Stellen vorbehalten, zunächst einmal nicht berührt.[17]

In diesem Zusammenhang wird teilweise auch das Modell einer digitalen Gewaltenteilung als Marktverantwortung vorgeschlagen.[18] Da die tatsächlichen Fä-

---

[11] Vgl. statt vieler *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 22; vgl. auch *Helm*, Rechtspflicht zur Privatisierung, S. 132 ff.

[12] So aber die These des sogenannten „Subsidiaritätsprinzips", dazu *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 65 ff. Zur fehlenden rechtlichen Verbindlichkeit statt vieler m.w.N. *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 22.

[13] BVerwG NJW 1995, 2938 (2939).

[14] Wie etwa beim für verfassungswidrig befundenen staatlichen Monopol für Sportwetten, BVerfG NJW 2006, 1261 oder beim verfassungsgerichtlich gehaltenen Arbeitsvermittlungsmonopol, BVerfGE 21, 245.

[15] Skeptisch *Heckmann/Bernhardt*, Digitale Gewaltenteilung als Marktverantwortung, S. 16 f.; *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Vorbemerkung.

[16] So auch *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 39. Vgl. *Burgi*, NZBau 2001, 64 (65).

[17] Anders ohne Begründung *Heckmann/Bernhardt*, Digitale Gewaltenteilung als Marktverantwortung, S. 6 für melderechtliche Vorschriften, die eine Datenverarbeitung bestimmten behördlichen Stellen vorbehalten.

[18] *Heckmann/Bernhardt*, Digitale Gewaltenteilung als Marktverantwortung, passim; *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 61 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

higkeiten im Bereich IT vor allem bei privaten Unternehmen vorhanden seien, müsse sich der Staat mit diesen zusammenschließen, um etwa die Funktionsfähigkeit von staatlichen IT-Strukturen sicherzustellen. Dies schließe auch eine Marktverantwortung des Staates ein, der er mittels Wettbewerbs- und Beschaffungsmaßnahmen sowie einer Einbeziehung privater Unternehmen nachzukommen habe. Indes erscheint es nicht angebracht, aus einer Beschreibung des tatsächlichen Ist-Zustands normative Vorgaben abzuleiten. Forderungen nach einer digitalen Gewaltenteilung mögen politischer Natur sein, rechtlich begründen lassen sie sich kaum; denn maßgeblich dafür bleibt grundsätzlich, dass der Staat eigenverantwortlich entscheiden kann, ob er eine Leistung an sich selbst erbringt oder sie sich am Markt beschafft, dass ihn keine Privatisierungspflicht trifft und dass es in solchen Konstellationen in aller Regel zu keiner Beeinträchtigung des Art. 12 Abs. 1 GG kommt.[19]

3. Unterscheidung zwischen Aufgabe und Aufgabenfeld

Die Anforderungen an eine Einbindung Privater in die Wahrnehmung öffentlicher Aufgaben lassen sich stets nur mit Blick auf die Besonderheiten des jeweiligen Sachbereichs bestimmen. Dabei ist es insbesondere hilfreich, zwischen der konkreten Aufgabe und dem Aufgabenfeld zu unterscheiden, welchem die betreffende Aufgabe thematisch zuzuordnen ist.[20] Dass der Staat in einem bestimmten Aufgabenfeld (z. B. Strafvollzug) tätig ist, bedeutet etwa noch nicht, dass er sämtliche Aufgaben in diesem Bereich übernimmt oder übernehmen muss (z. B. Betrieb einer Anstaltsküche).[21] Umgekehrt müssen bei der Privatisierung bestimmter Aufgaben mögliche Rückwirkungen im übergeordneten Aufgabenfeld stets mit bedacht werden.

Die Unterscheidung zwischen Aufgabe und Aufgabenfeld ist gerade für den Gegenstand des vorliegenden Gutachtens von besonderer Bedeutung. Einerseits ist die Verarbeitung staatlich erhobener Daten eine eigenständige, abgrenzbare Aufgabe. Andererseits ist sie nicht vollständig von dem übergeordneten Aufgabenfeld zu trennen, innerhalb dessen der Staat die Daten ursprünglich – und in Wahrnehmung einer Staatsaufgabe – erhoben hat.

[19] Zu letzterem ausführlicher noch unten D. III.

[20] Zur Unterscheidung zwischen Aufgabe und Aufgabenfeld *Burgi*, Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, Gutachten für den 67. DJT, S. 53 ff.

[21] Vgl. zu diesem Aufgabenfeld mit weiteren Beispielen etwa *Wissenschaftlicher Dienst des Bundestages*, Privatisierung im Strafvollzug, S. 3 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

II. Obligatorische Staatsaufgaben

Zwar verzichtet das Grundgesetz darauf, bestimmte Aufgaben ausdrücklich und exklusiv dem Staat zuzuweisen und Private so von ihrer Wahrnehmung auszuschließen.[22] Dies bedeutet allerdings nicht, dass sich der Verfassung keinerlei aufgabenbezogene Privatisierungsgrenzen entnehmen ließen. Jedenfalls im Ergebnis besteht, wie eingangs bereits angedeutet,[23] weitgehend Einigkeit, dass ein gewisser unveräußerlicher Kernbestand staatlicher Aufgaben existiert, die häufig als „obligatorische" Staatsaufgaben bezeichnet werden.[24] Hieraus ergeben sich – zumindest mittelbar – auch erste Grenzen für die Zulässigkeit einer Übertragung von Datenverarbeitungsaufgaben auf Private.

1. Bereiche und Reichweite obligatorischer Staatsaufgaben

Obligatorische Staatsaufgaben finden sich in Aufgabenfeldern, die elementare staatliche Funktionen zum Gegenstand haben.[25] Klassischerweise werden hier unter anderem Gesetzgebung und Justiz, die Gewährleistung innerer und äußerer Sicherheit, die Strafverfolgung und die Finanzverwaltung genannt.[26] Wegen des unmittelbaren Menschenwürdebezugs[27] spricht ferner einiges dafür, auch die Gewährleistung unverzichtbarer Sozialleistungen („Existenzminimum") als obligatorische Staatsaufgabe zu begreifen.

Auch wenn ein Aufgabenfeld obligatorische Staatsaufgaben beinhaltet, kann es in Teil- und Randbereichen einer Mitwirkung Privater zugänglich sein – man denke nur an private Sicherheitsdienste.[28] Unzulässig wäre aber jedenfalls eine vollständige Privatisierung des gesamten Bereiches.[29] Darüber hinaus ist auch der Kernbereich der oben genannten Aufgabenfelder einer Privatisierung verschlossen. Dieser wird etwa

[22] Dazu soeben C. I. 2.

[23] Vgl. oben C. I. 1.

[24] *Burgi*, Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, Gutachten für den 67. DJT, S. 53 ff.; *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 27 ff. definiert innerhalb der „obligatorischen" Staatsaufgaben noch die Teilmenge der „ausschließlichen" Staatsaufgaben; *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 102: „originäre" Staatsaufgaben; *Peters*, in: Dietz/Hübner (Hrsg.), FS II Nipperdey, S. 877 (892): „echte" Staatsaufgaben.

[25] Vgl. *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 27 Rn. 31; *Thiele*, Der Staat 49 (2010), 274 (279).

[26] Vgl. *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 28; *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 102; *Peters*, in: Dietz/Hübner (Hrsg.), FS II Nipperdey, S. 877 (892); *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 95; *Schuppert*, Staatswissenschaft, S. 292.

[27] BVerfGE 125, 175.

[28] *Voßkuhle*, VVDStRL 62 (2003), 266 (275); näher hierzu *C. Ernst*, NVwZ 2015, 333.

[29] *Isensee*, in: ders./P. Kirchhof (Hrsg.), HStR IV, § 73 Rn. 28.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

dann betroffen sein, wenn die Aufgabenwahrnehmung typischerweise auf den Einsatz physischer Gewalt angewiesen ist, wie es etwa bei der Polizei der Fall ist.[30] Allgemeiner kommt es darauf an, inwieweit eine Einzelaufgabe „typusprägend" für das jeweilige Gebiet (also etwa die Gesetzgebung oder die Justiz) ist.[31] Der Staat darf sich durch die Entäußerung einer Aufgabe bei wertender Betrachtung nicht der unmittelbaren Kontrolle über eine seiner zentralen Funktionen entledigen.

2. Datenverarbeitung selbst als obligatorische Staatsaufgabe

Es existiert keine allgemeine Regel, nach der der Umgang mit staatlich erhobenen oder zu staatlichen Zwecken verwendeten Daten stets als obligatorische Staatsaufgabe einzuordnen wäre.

a) Voraussetzungen für die Annahme einer obligatorischen Staatsaufgabe

Um eine Verarbeitung von Daten selbst als obligatorische Staatsaufgabe einzuordnen, kommt es entscheidend auf den Kontext der Datenerhebung und -verarbeitung an. Dabei ist insbesondere zu berücksichtigen, dass die Erhebung und Verwaltung von Daten regelmäßig kein Selbstzweck ist. Sie erfüllt zumeist eine bloß unterstützende Funktion innerhalb eines Aufgabenfeldes und bildet kaum einmal dessen unmittelbaren Gegenstand.

Dennoch ist es durchaus denkbar, dass Datenverarbeitungsprozesse schon für sich genommen als obligatorische Staatsaufgaben einzuordnen sind. Denn es ist zumindest nicht von vornherein ausgeschlossen, dass die Datenverarbeitung selbst den Kern eines Aufgabenfeldes bildet.[32] In diesen Konstellationen sind die Daten also nicht lediglich Annex zu einer Staatsaufgabe, sondern selbst ihr unmittelbarer Gegenstand.

b) Beispiel: Meldewesen

Im Rahmen des Meldewesens erhebt der Staat unterschiedliche Daten über seine Bürger. Erste Meldepflichten entwickelten sich bereits im 16. Jahrhundert, mit dem Ziel, die öffentliche Ordnung aufrecht zu halten.[33] Heutzutage erfüllt das Meldewesen eine ganz grundlegende Vorleistungsfunktion für zahlreiche andere – und

[30] *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 20.

[31] Vgl. *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 17, für die in Art. 87 ff. GG genannten Aufgaben, der Gedanke ist aber darüber hinaus verallgemeinerungsfähig.

[32] *Petri/Dorfner*, ZD 2011, 122 (127).

[33] *Marenbach*, Die informationellen Beziehungen zwischen Meldebehörde und Polizei in Berlin, S. 30 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

häufig belastende – staatliche Maßnahmen.[34] Obwohl die Meldedaten damit auch eine unterstützende Funktion für eine Vielzahl anderer Verwaltungsaufgaben erfüllen, sind sie – anders als typische Daten im Verwaltungsgebrauch sonst – zusätzlich unmittelbarer Gegenstand der eigenständigen Aufgabe, ein staatliches Meldewesen zu unterhalten. Da die Datenerhebung im Meldewesen nicht spezifisch auf die Wahrnehmung einer bestimmten Aufgabe ausgerichtet ist, sondern ohne konkreten Anlass im Rahmen einer Vielzahl von Staatsaufgaben Relevanz entfalten kann (aber auch nicht muss), kann zwischen der eigenständigen Datenerhebung und -verarbeitung im Meldewesen sowie der Wahrnehmung weiterer Verwaltungsaufgaben unterschieden werden. Die Erlangung staatlichen Wissens über die Bürger ist ungeachtet sonstiger Verwaltungsaufgaben schon eine staatliche Aufgabe. Ausnahmsweise wird man also annehmen müssen, dass „die Datenverarbeitung selbst die primär zu erfüllende staatliche Aufgabe“ ist.[35]

Auch wenn das Meldewesen bei den „klassischen“ Aufzählungen obligatorischer Staatsaufgaben nicht genannt wird, spricht doch einiges für eine solche Einordnung.[36] Neben der Bedeutung der Meldedaten für die Erfüllung einer Vielzahl anderer (obligatorischer) Staatsaufgaben kann dafür auch auf die Sensibilität der Meldedaten verwiesen werden. Das Melderegister enthält umfassende und für den einzelnen Bürger potenziell intime oder gar sicherheitsrelevante Informationen. Nach § 3 BMG werden unter anderem Daten zur Wahlberechtigung sowie Passversagungsgründe gespeichert. Auch Informationen, die auf den ersten Blick im Alltag häufig bekannt sind, wie solche zu Geschlecht und Personenstand oder Wohnort können im Einzelfall eine erhebliche Sensibilität aufweisen oder bei Bekanntwerden zu Gefahren führen. So lassen sich dem Melderegister auch vergangene Geschlechtsumwandlungen entnehmen oder eine Unterkunft von Frauen in Frauenhäusern (wobei letzteres nach § 52 Abs. 1 Nr. 4 BMG mit einem bedingten Sperrvermerk zu versehen ist). Hier deutet sich schon an, dass es zu Überschneidungen zwischen den einzelnen Begründungssäulen für den Grundsatz digitaler Souveränität kommen kann.[37]

Ordnet man das Meldewesen also als privatisierungsfeste obligatorische Staatsaufgabe ein, so dürfte auch eine Auslagerung der Meldedaten an Private grundsätzlich unzulässig sein, weil es sich hierbei gerade um den Aufgabenkern handelt.[38] Dahinter steht der Grundsatz der digitalen Souveränität.

---

[34] *Heckmann/Braun*, BayVBl. 2009, 581 (584 f.); vgl. *Conrad/Strittmatter*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 22 Rn. 203.

[35] *Heckmann/Braun*, BayVBl. 2009, 581 (584).

[36] *Knemeyer*, Juridica International 2009, 22 (24) nennt das Pass- und Meldewesen explizit als weitestgehend privatisierungsfeste staatliche (bzw. kommunale) Aufgabe.

[37] Vgl. zur Gewährleistungsverantwortung nach außen aufgrund besonders sensibler personenbezogener Daten unten C. III. 3. b) aa).

[38] Zwar nicht so weitgehend, aber ebenfalls restriktiv *Heckmann/Braun*, BayVBl. 2009, 581 (586).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Als anschauliches Gegenbeispiel kann das Archivwesen herangezogen werden. Nach § 3 Abs. 1 BArchG ist es Aufgabe des Bundesarchivs, das Archivgut des Bundes, also Unterlagen von bleibendem Wert (§ 1 Nr. 2 BArchG) auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten. Wie auch beim Meldewesen ist die Informationskonservierung bzw. Datenverarbeitung selbst die zu erfüllende staatliche Aufgabe. Im Falle des Bundesarchivs treten daneben die Aufgaben, die Benutzung des Archivguts und deren wissenschaftliche Veröffentlichung zu ermöglichen.[39] Im Falle der Digitalisierung von archivierten Unterlagen kann sich die Frage stellen, ob private IT-Dienstleister in die Aufgabenwahrnehmung einbezogen werden dürfen. Dafür sprechen die weiteren Aufgaben des Bundesarchivs, die neben die Aufgabe der Sicherung der Unterlagen treten. Anders als beim Meldewesen sollen die betroffenen Daten grundsätzlich von vornherein verbreitet und durch (private) Dritte genutzt werden. Auch war bis vor 30 Jahren umstritten, ob es für das Archivwesen überhaupt eine gesetzliche Grundlage bedurfte und letztendlich waren es Rechtsgüterkonflikte, die den Ausschlag gaben.[40] Vor diesem Hintergrund scheint es sich nicht um eine Aufgabe zu handeln, die zwingend durch den Staat wahrzunehmen ist. Gleichwohl erscheint es im Einzelfall nicht ausgeschlossen, dass eine andere Facette des Grundsatzes digitaler Souveränität zu einem Ausschluss privater IT-Dienstleister führen kann.

3. Datenverarbeitung als integraler Bestandteil obligatorischer Staatsaufgaben

Die Auslagerung einer Datenverarbeitung an Private ist darüber hinaus auch dann unzulässig, wenn diese integraler Bestandteil einer obligatorischen Staatsaufgabe ist.

a) Voraussetzungen für die Annahme eines integralen Bestandteils

Datenverarbeitung kann als integraler Bestandteil einer obligatorischen Staatsaufgabe angesehen werden, wenn die Wahrnehmung einer solchen Aufgabe mit den betreffenden Daten „steht und fällt“. Die Datenverarbeitung bildet eine Teilaufgabe oder Teilfunktion innerhalb des Aufgabenfeldes.[41] Diese Fallgruppe liegt gewissermaßen eine Ebene hinter der soeben skizzierten: Die Datenverarbeitung bildet zwar nicht selbst den „typusprägenden Kern“[42] eines nicht (vollständig) privatisierungsfähigen Aufgabenfeldes. Sie wird aber vom Privatisierungsverbot hinsichtlich

[39] S. *Becker/Oldenhage*, BArchG, § 1 Rn. 19 f.

[40] S. *Becker/Oldenhage*, BArchG, § 1 Rn. 3.

[41] In der Sache unterstützt die Datenverarbeitung durch die Verwaltung regelmäßig die Wahrnehmung von Verwaltungsaufgaben. Nicht weiter vertieft werden soll an dieser Stelle, ob daher die Datenverarbeitung selbst als (Teil-)Funktion oder als Teilaufgabe bezeichnet werden kann.

[42] Vgl. oben C. II. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

einer Kernaufgabe erfasst, weil und soweit sie für deren Wahrnehmung unverzichtbar ist und eine konstituierende Wirkung aufweist.[43]

Dieses gleichsam akzessorische Privatisierungsverbot beruht auf der Erkenntnis, dass die ständige Verfügbarkeit und Verarbeitung bestimmter Daten für die Wahrnehmung vieler obligatorischer Staatsaufgaben heute essenziell ist. Schon die schlichte Bereitstellung ausreichender Ressourcen zur Datenverarbeitung kann für die Wahrnehmung obligatorischer Staatsaufgaben und -funktionen zwingend notwendig sein, etwa im Bereich der Gerichtsverwaltung.[44] In manchen Bereichen sind Daten auch seit jeher elementarer Bestandteil der Aufgabenwahrnehmung und haben ihre besondere Bedeutung nicht erst durch das Aufkommen digitaler Informationstechnologien erhalten. Dies ist besonders augenfällig im Bereich der Abgabenerhebung. Diese ist – weitestgehend[45] – eine obligatorische Staatsaufgabe, weil sie im Zentrum der Finanzverwaltung steht und die Handlungsfähigkeit des Staates sichert; zugleich funktioniert sie als EDV-gestützte Massenverwaltung.[46] Auch insoweit kann sich das Privatisierungsverbot hinsichtlich der Aufgabe als solcher im Einzelfall auch auf hierfür unverzichtbare Datenbestände erstrecken.

Hier zeigt sich besonders deutlich, dass die Kategorie „integraler Bestandteil einer obligatorischen Staatsaufgabe“ eng mit der noch näher zu betrachtenden staatlichen „Gewährleistungsverantwortung nach innen“ zusammenhängt. Der Unterschied besteht im Wesentlichen darin, dass die Unverzichtbarkeit von Daten für die Wahrnehmung einer obligatorischen Staatsaufgabe die weitere Abwägung entbehrlich macht – Privaten darf schon dann ein Zugriff auf die Daten nicht ermöglicht werden. Die Übergänge sind insofern allerdings fließend und eine integrale Funktion von Daten für die Aufgabenwahrnehmung sollte nicht vorschnell angenommen werden. Auch im Bereich einer Abwägung gilt aber: Je zentraler ein Datenbestand für die Wahrnehmung einer obligatorischen Staatsaufgabe ist, desto weniger kommt eine Privatisierung in Betracht.

---

[43] Vgl. *Petri/Dorfner*, ZD 2011, 122 (127).

[44] Vgl. *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 37: „Die Gerichtsverwaltung ermöglicht die Funktionsfähigkeit einer anderen Staatsgewalt überhaupt erst.“

[45] Die Einbeziehung Privater in Randbereichen und namentlich die Indienstnahme der Arbeitgeber bei der Abführung der Lohnsteuer (darauf hinweisend etwa *Hengstschläger*, VVDStRL 54 (1995), 165 [175]) stellt die Einordnung als obligatorische Staatsaufgabe nicht in Frage.

[46] Vgl. *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 34 f.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

b) Beispiele: Elektronische Prozessakten bei den Zivilgerichten, § 298a ZPO, und Einsatz elektronischer Wahlgeräte

Nach § 298a Abs. 1, 1a ZPO können Prozessakten elektronisch geführt werden.[47] Der Gesetzgeber hat mittlerweile durch das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017[48] festgelegt, dass die Prozessakten ab dem 1. Januar 2026 elektronisch zu führen sind. Dazu bestimmen die Bundesregierung und die Landesregierungen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Akten geführt werden sowie die hierfür geltenden organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Aufbewahrung der elektronischen Akten. Bislang haben Baden-Württemberg,[49] Bayern,[50] Brandenburg,[51] Mecklenburg-Vorpommern,[52] Nordrhein-Westfalen,[53] Rheinland-Pfalz[54] und Schleswig-Holstein[55] von der Verordnungsermächtigung Gebrauch gemacht.

Für die Frage, wer mit dem Führen der elektronischen Prozessakten zu betrauen ist, enthält die bundesgesetzliche Regelung keinen Hinweis. Der überwiegende Teil der Verordnungen enthält zwar Sicherheitsanforderungen, jedoch keine ausdrücklichen Regelungen, wer die elektronischen Prozessakten führt.[56] Einzig die bayeri-

[47] Daneben haben die Bundesländer unter Verweis auf § 130a ZPO Verordnungen zum elektronischen Rechtsverkehr, also der Möglichkeit Schriftsätze als elektronisches Dokument bei Gericht einzureichen, Gebrauch gemacht. Der noch nicht in Kraft getretene § 130d ZPO verpflichtet Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts hierzu ab dem 1. Januar 2022. Vgl. die Zusammenstellung http://www.justiz.de/elektronischer_rechts verkehr/index.php; vgl. *M. Huber*, in: Musielak/Voit (Hrsg.), ZPO, § 298a Rn. 2, 4.

[48] BGBl. I S. 2208.

[49] Verordnung des Justizministeriums zur elektronischen Aktenführung bei den Gerichten vom 29. 3. 2016, BWGBl. S. 265.

[50] Verordnung über den elektronischen Rechtsverkehr bei den ordentlichen Gerichten vom 15. 12. 2006, BayGVBl. S. 1084.

[51] Verordnung zur elektronischen Aktenführung bei den Gerichten vom 3. 1. 2019, BbgGVBl. II Nr. 2.

[52] Verordnung zur elektronischen Aktenführung bei den Gerichten vom 4. 8. 2018, GVOBl. M-V S. 307.

[53] Verordnung zur elektronischen Aktenführung bei den Gerichten der ordentlichen Gerichtsbarkeit im Land Nordrhein-Westfalen in Zivil- und Familiensachen vom 16. 10. 2018, GV. NRW. S. 578.

[54] Landesverordnung über die elektronische Aktenführung bei den Gerichten in Rheinland-Pfalz vom 9. 5. 2018, RhPfGVBl. S. 125.

[55] Landesverordnung über die elektronische Aktenführung in der Justiz vom 11. 3. 2019, GVOBl. S-H S. 61.

[56] § 5 VO BW weist dem Justizministerium eine maßgebliche Rolle zu, wobei unklar bleibt, ob dieses zwingend die elektronischen Akten selbst führen muss, um den gesetzlichen Anforderungen gerecht zu werden; vgl. ansonsten § 5 VO Bbg; §§ 4 f. VO M-V; § 4 VO NRW; § 4 VO RhPf mit Verweis auf § 64 Abs. 2 Grundbuchverfügung; §§ 5 f. VO S-H.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

sche E-Rechtsverkehrsverordnung Justiz (ERVV Ju)[57] bestimmt in § 5 Abs. 1, dass die Datenverarbeitung durch das Landesamt für Steuern zu erfolgen hat.

Die Rechtsprechung als eine klassische Staatsgewalt kann als obligatorische Staatsaufgabe eingeordnet werden. Daten und Informationen als Bestandteile von Akten bilden für die Tätigkeit und Funktionsfähigkeit der Rechtsprechung seit jeher einen elementaren und integralen Bestandteil und stehen somit im Zentrum der Staatsaufgabe Rechtsprechung. Bei der Bewältigung einzelner Gerichtsverfahren spielen die Akteninhalte eine überragende Rolle.[58] Ihre besondere Bedeutung hat sich nicht erst ergeben, als digitale Informationstechnologien die Möglichkeit dazu boten, sondern ist traditionell ein essenzieller Bestandteil der Rechtsprechungstätigkeit über die Jahrhunderte hinweg gewesen.

Für die zukünftigen Verordnungen in den Bundesländern, die bislang keine Regelungen getroffen haben, wer für das Führen elektronischer Prozessakten zuständig ist, sind diese Grundsätze zu beachten. Es ist deshalb sicherzustellen, dass die elektronischen Prozessakten in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben.

Ähnliches gilt für den Bereich der Sozialverwaltung[59] und auch in anderen Gebieten ist die Einordnung von bestimmten Datenbeständen als integrale Bestandteile obligatorischer Staatsaufgaben denkbar, etwa im Kernbereich der inneren und äußeren Sicherheit (Datenbanken der Polizei, Geheimdienste oder Streitkräfte) oder der Strafverfolgung (BZR, MeSta).

Auch im Falle des Einsatzes elektronischer Wahlgeräte bei den Wahlen zu den parlamentarischen Volksvertretungen kann die Datenverarbeitung als integraler Bestandteil des verfassungsrechtlich vorgesehenen Wahlvorgangs verstanden werden. Das Bundesverfassungsgericht hat in der Vergangenheit an die elektronische Ausgestaltung des Wahlakts besondere Voraussetzungen gestellt. Der Grundsatz der Öffentlichkeit der Wahl setzt voraus, dass sich die Wähler vom korrekten Ablauf der Wahl überzeugen können.[60] Dies sah das Bundesverfassungsgericht aufgrund der eingesetzten Wahlcomputer nicht als gesichert an, obwohl diese im Einklang mit den einfachgesetzlichen Wahlregelungen standen. Zur Einbindung Privater nahm es zwar nicht Stellung, doch die getroffene Entscheidung kann auch im Lichte des Grundsatzes digitaler Souveränität verstanden werden. Denn bei der Verarbeitung der im

[57] VO vom 15. 12. 2006, GVBl. S. 1084.

[58] Hier mag es Unterschiede zu Strafverfahren geben, bei denen das Gericht nach § 261 StPO über das Ergebnis der Beweisaufnahme nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung entscheidet. Zur Situation im Strafverfahren, für das auch die Gewährleistungsverantwortung nach außen eine maßgebliche Rolle spielt, vgl. unten C. III. 3. b) cc).

[59] Zur Einordnung als obligatorische Staatsaufgabe zumindest im Bereich der Existenzsicherung oben C. II. 1. Zur Bedeutung einer Gewährleistungsverantwortung nach außen für die Sozialverwaltung unten C. III. 3. b) cc).

[60] BVerfGE 123, 39 (68 f.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

eigentlichen Wahlakt anfallenden Daten (vor allem, aber nicht ausschließlich) im Rahmen einer möglichen elektronischen Wahl handelt es sich aufgrund der hervorgehobenen Bedeutung dieser Daten für das Wahlergebnis um einen integralen Bestandteil der demokratischen Staatsfunktion Wahlen. Ebenso wie die wesentlichen Schritte einer Wahlhandlung und die Ergebnisermittlung einer besonderen öffentlichen Kontrolle zugänglich sein müssen, darf nicht einzelnen Privaten eine Zugriffsmöglichkeit auf die Daten der Wahlhandlung und Wahlergebnisse eingeräumt werden. Dies ergibt sich nicht nur aus dem zwingend staatlichen Charakter der Wahlen, sondern zusätzlich auch daraus, dass sich private Zugriffsmöglichkeiten nicht mit dem Grundsatz der Öffentlichkeit der Wahl vereinbaren lassen.

c) Abgrenzung zur Datenverarbeitung als bloßer Annex zu (obligatorischen) Staatsaufgaben

In der überwiegenden Zahl der Fälle wird eine Datenverarbeitung weder selbst als obligatorische Staatsaufgabe anzusehen sein, noch werden Datenbestände derart zentral für eine solche Aufgabe sein, dass sie von einem diesbezüglichen Privatisierungsverbot erfasst werden. Stattdessen ist die Verarbeitung von Daten, die bei der Wahrnehmung auch obligatorischer Staatsaufgaben anfallen, regelmäßig nur ein bloßer Annex, eine Teilfunktion oder Teilaufgabe innerhalb des Aufgabenfeldes, die aber außerhalb von dessen Kern liegt.

In diesem großen Bereich ist eine Betrauung Privater mit der Datenverarbeitung zumindest unter dem Gesichtspunkt der Staatsaufgabenlehre grundsätzlich zulässig. Die Datenübertragung kann allerdings gleichwohl im Hinblick auf eine staatliche Gewährleistungsverantwortung oder aufgrund eines Vertrauens in den staatlichen Einsatz digitaler Informationstechnologien unzulässig sein; dies wird noch zu erörtern sein.

Soweit die Datenverarbeitung lediglich einen Annex zu (obligatorischen) Staatsaufgaben darstellt, ist eine Einbindung Privater als bloße Hilfspersonen (sog. Verwaltungshelfer), die keinerlei Hoheitsbefugnisse ausüben und deren Aufgaben eher vorbereitenden und durchführenden Charakter haben, im Ausgangspunkt unbedenklich.[61] Ein klassisches Beispiel hierfür ist der private Abschleppunternehmer. Vergleichbare Hilfstätigkeiten im Bereich der Datenverwaltung können etwa die bloße Speicherung auf privaten Servern oder eine automatisierte Verarbeitung sein.[62] Derartige Aufgaben auf private Anbieter auszulagern, ist jedenfalls, sofern es sich hierbei nicht um einen integralen Bestandteil einer obligatorischen Staatsaufgabe handelt, sondern einen bloßen Annex, nicht schlichtweg unzulässig. Die Probleme verschieben sich vielmehr auf eine angemessene Auswahl und Kontrolle der Verwaltungshelfer, mithin auf Fragen der Wahrnehmung staatlicher Gewährleistungs-

[61] Allgemein statt vieler *Burgi*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 75 Rn. 7; für den Bereich der Datenverwaltung *Ulmer*, CR 2003, 701 (703).

[62] *Ulmer*, CR 2003, 701 (704).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

verantwortung.[63] Diese kann allerdings im Bereich der Datenverwaltung mit besonderen Schwierigkeiten verbunden sein.[64]

Auch im weiten Feld der nicht obligatorischen Staatsaufgaben können staatliche Daten prinzipiell in einen privaten Herrschaftsbereich verbracht werden. Die Verfassung schreibt grundsätzlich keine bestimmte Aufgabenverteilung zwischen Staat und Privatwirtschaft vor und steht einer Beteiligung Privater an der Erfüllung öffentlicher Aufgaben offen gegenüber.[65] Wie problematisch eine konkrete Aufgabenübertragung an Private im Hinblick auf Daten ist, hängt maßgeblich davon ab, ob dem Auftragnehmer ein eigenverantwortlicher Umgang mit den Daten gestattet wird.[66] Je stärker dies der Fall ist, desto eher kann die Tätigkeit des Privaten als „hoheitlich" einzustufen sein und dem Funktionsvorbehalt des Art. 33 Abs. 4 GG unterliegen.[67] Zudem wird dann der Bereich der Auftragsverarbeitung und ihrer Privilegierung nach Art. 24 ff. DSGVO, § 64 BDSG verlassen.[68]

III. Gewährleistungsverantwortung

Der Grundsatz digitaler Souveränität kann auch auf das Modell der Gewährleistungsverantwortung zurückgeführt werden.

1. Konzept der Gewährleistungsverantwortung

Das Konzept der Gewährleistungsverantwortung reagiert auf die erheblichen Probleme der Staatsaufgabenlehre, „staatliche" und „private" Aufgaben normativ zuverlässig voneinander abzugrenzen. An die Stelle eines gegenstandsbezogenen Aufgabendenkens tritt der flexiblere Verantwortungsgedanke, der Arbeitsteilungen zwischen öffentlichem und privatem Sektor bei der Aufgabenwahrnehmung besser abbilden und verarbeiten kann.[69] Insofern werden namentlich drei Verantwortungsstufen unterschieden:[70] Eine Erfüllungsverantwortung trifft den Staat dort, wo

[63] Statt vieler *Voßkuhle*, VVDStRL 62 (2003), 266 (296).

[64] Dazu sogleich C. III. 2.

[65] Siehe dazu bereits oben C. I. 2.

[66] *Ulmer*, CR 2003, 701.

[67] Näher *Ulmer*, CR 2003, 701 (703).

[68] Zum Zusammenhang zwischen Art. 33 Abs. 4 GG und § 11 a.F. BDSG vgl. etwa *Petri*, in: Simitis (Hrsg.), BDSG, § 11 Rn. 9 f.

[69] *Voßkuhle*, in: Schuppert (Hrsg.), Jenseits von Privatisierung und „schlankem" Staat, S. 47 (57); *Franzius*, Der Staat 42 (2003), 493 (504 f.); *Schuppert*, Staatswissenschaft, S. 289 ff.

[70] Hierzu etwa *Hoffmann-Riem*, in: Kirchhof/Lehner/Raupach/Rodi (Hrsg.), FS Vogel, S. 47 ff.; *Schuppert*, in: ders. (Hrsg.), Der Gewährleistungsstaat – Ein Leitbild auf dem Prüfstand, S. 11 (25 f.); *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 150 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

er Aufgaben eigenhändig wahrnimmt. Hierzu ist er – außerhalb der oben diskutierten obligatorischen Staatsaufgaben – indes grundsätzlich nicht verpflichtet, vielmehr kann er prinzipiell auch Private in die Aufgabenwahrnehmung einbeziehen. Auch dann trifft den Staat aber weiterhin eine Gewährleistungsverantwortung dahingehend, dass er die Gemeinwohlverträglichkeit der privaten Aufgabenerfüllung sicherstellen muss. Erweist sich diese „mittelbare" Gemeinwohlsicherung im Einzelfall als nicht ausreichend, lebt die staatliche Erfüllungsverantwortung als Auffangverantwortung wieder auf – der Staat muss die Aufgabe dann „zurückholen" und wieder selbst wahrnehmen.

Der „Gewährleistungsstaat" gilt inzwischen vielfach als Leitbild des modernen Staates.[71] Mit der Einbindung Privater verbindet sich dabei insbesondere die Hoffnung einer effizienteren Aufgabenerfüllung.[72] Freilich ist das Gewährleistungskonzept auch mit besonderen Schwierigkeiten und Gefahren verbunden. Die zumeist hervorgehobene Erkenntnis, dass eine Einbindung Privater grundsätzlich möglich ist, droht den Blick auf die Probleme bei der konkreten Umsetzung zu verstellen.[73]

Dies gilt bereits auf normativer Ebene. Zwar lässt sich regelmäßig gut begründen, dass eine staatliche Gewährleistungsverantwortung für eine Aufgabe besteht, etwa aufgrund verfassungsrechtlicher Staatszielbestimmungen und grundrechtlicher Schutzpflichten. Allerdings geht mit diesen Verfassungsprinzipien immer die Frage einher, wie diese Verantwortung konkret wahrzunehmen ist. Im Vergleich zu einer unmittelbar staatlichen Aufgabenwahrnehmung sinkt die Steuerungskraft des Verfassungsrechts;[74] namentlich die Grundrechte der von der Aufgabe betroffenen Bürger sind nur noch in ihrer Schutzdimension relevant.[75] Angesichts der erheblichen verfassungsrechtlichen Spielräume ist staatliche Gewährleistungsverantwortung primär (gesetzgeberische) Rechtsetzungsverantwortung.[76]

Auf der tatsächlichen Ebene stellt sich insbesondere die Frage, inwiefern der Staat – sei es durch Erlass neuer oder aufgrund bestehender Regelungen – praktisch in der Lage ist, seiner Verantwortung nachzukommen.[77] Probleme bereitet insbesondere die Sicherstellung einer effektiven Lenkung und Kontrolle der privaten Akteure, die zu Recht als „Achillesferse" des Gewährleistungskonzepts bezeichnet wurde.[78] Die

[71] Vgl. dazu die Beiträge in Schuppert (Hrsg.), Der Gewährleistungsstaat – Ein Leitbild auf dem Prüfstand; ferner *Franzius*, Der Staat 42 (2003), 493 (504 f.).

[72] Statt vieler *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 93 f.

[73] Vgl. *Röhl*, Die Verwaltung, Beiheft 2, 1999, 33 (53 f.).

[74] Näher *Voßkuhle*, VVDStRL 62 (2003), 266 (291 ff.).

[75] Anschaulich *Franzius*, Der Staat 42 (2003), 493 (508), der ausführt, dem Bürger käme so „der Staat als Grundrechtsadressat abhanden"; *Kämmerer*, Privatisierung, S. 453: „Verflachen" des Grundrechtsschutzes.

[76] *Voßkuhle*, VVDStRL 62 (2003), 266 (327).

[77] *Röhl*, Die Verwaltung, Beiheft 2, 1999, 33 (53 f.).

[78] *Voßkuhle*, VVDStRL 62 (2003), 266 (320 ff.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Optimierung der Steuerung der privaten Aufgabenträger ist geradezu zwangsläufig ein Verfahren von „Trial-and-Error".[79] Daher sind die Gefahren von Fehlschlägen bereits im Vorfeld einer (Teil)Privatisierung umfassend und sorgfältig zu prüfen. In der Folge muss die Aufgabenerfüllung fortlaufend kontrolliert und evaluiert werden und es muss sichergestellt werden, dass eine effektive Nachsteuerung möglich ist, falls es zu Problemen kommt.[80] Schließlich ist dafür Sorge zu tragen, dass der Staat für den Fall des Scheiterns des Privatsektors seine Auffangverantwortung auch tatsächlich wahrnehmen kann, was durchaus erhebliche praktische Schwierigkeiten bereiten kann, wenn Expertise und Personal erst einmal aus der Verwaltung abgewandert sind. Die skizzierten allgemeinen Herausforderungen können sich bereichsspezifisch ganz unterschiedlich darstellen[81] und sind – wie jetzt zu zeigen sein wird – gerade im Bereich der Datenverarbeitung mit besonderen Schwierigkeiten verbunden.

2. Besondere Herausforderungen bei IT-Outsourcing und Datenübermittlung in einen privaten Hoheitsbereich

Das Entlassen von Daten aus einem öffentlich-rechtlichen Hoheitsbereich und das zumindest mittelbare Ermöglichen eines privaten Zugriffs auf die Daten findet häufig im Rahmen von IT-Outsourcing statt. Bei diesem bedient sich ein Träger staatlicher Gewalt dem Angebot eines privaten IT-Dienstleisters. Dies geschieht regelmäßig in der Hoffnung, die eigenen IT-Kosten zu senken und gleichzeitig eine privatwirtschaftlich erprobte Lösung zu erhalten.[82] Um welche Dienstleistungen es sich konkret handelt, ist dabei angesichts der Datenübermittlung an einen Privaten und dessen damit einhergehender Zugriffsmöglichkeit von nachrangiger Bedeutung.[83] Von besonderer Relevanz sind hingegen Besonderheiten, die gerade beim Umgang mit Daten bestehen und deren Konsequenzen für die Ausfüllung einer Gewährleistungsverantwortung.[84]

---

[79] *Schulze-Fielitz*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR I, § 12 Rn. 156.

[80] *Voßkuhle*, VVDStRL 62 (2003), 266 (325 f.).

[81] Zur Notwendigkeit einer bereichsspezifischen Betrachtung *Voßkuhle*, VVDStRL 62 (2003), 266 (311).

[82] *Küchler*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 1 Rn. 343 ff.; *Gründer*, DuD 2016, 667 (667). Vgl. auch *Schubert*, Privatisierung des eGovernment, S. 65 ff.

[83] Vgl. oben B.

[84] *Debski*, DuD 2016, 659 (661), unterscheidet in dieser Hinsicht zwischen allgemeinen Geschäftsrisiken und spezifischen IT-Risiken.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

a) Tatsächliche Rahmenbedingungen für die Ausübung einer Gewährleistungsverantwortung bei IT-Outsourcing und Datenübermittlung in einen privaten Hoheitsbereich

Bei der Auseinandersetzung mit einer Gewährleistungsverantwortung im Bereich des IT-Outsourcings und der Datenübermittlung in einen privaten Hoheitsbereich müssen die spezifischen Eigenheiten des Umgangs mit Daten berücksichtigt werden. Spezifische Risiken, die beim Umgang mit Daten bestehen können, müssen dabei auf den Akt der Übertragung von Daten aus einem staatlichen in einen privaten Herrschaftsbereich bezogen werden, so dass es nicht allein um einzelne konkrete IT-Dienstleistungen wie die Nutzung einer Cloud oder bestimmte Datenverarbeitungsvorgänge geht.

aa) Spezifische Gefahren beim Verarbeiten von Daten

Im Datenschutzrecht und in der Literatur finden sich verschiedene Arten von Gefahren, die sich unmittelbar auf Daten beziehen.[85] Diese im Einzelnen vielfältigen Risiken können auf eine überschaubare Anzahl klassischer Schutzziele beschränkt werden.[86] Unter Berücksichtigung der Art. 4 Nr. 12, 32 Abs. 2 DSGVO und des früheren Art. 17 Abs. 1 RL 95/46/EG können die Risiken für Daten im Verhältnis von ursprünglichem Dateninhaber und IT-Dienstleister auf die vier Grundfälle Verfügbarkeit, Verfälschung, sachfremde Nutzung und Veröffentlichung zurückgeführt werden.[87] Dabei sollen die konkreten Gründe oder Fragen des Verschuldens für eine mögliche Realisierung der Risiken unerheblich bleiben.[88]

---

[85] *Debski*, DuD 2016, 659 (662 ff.); *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 17 (27). Vgl. auch die Anlage 1 zu § 9 BDSG sowie die Anlage 1 zur Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 VI BSIG, dazu *Grobauer*, DuD 2016, 17 (20).

[86] Vgl. *Hladjk*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 32 Rn. 8; *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 32 Rn. 22.

[87] Art. 4 Nr. 12 Datenschutz-Grundverordnung (VO 2016/679): „… Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".

Art. 17 I Datenschutzrichtlinie (RL 95/46/EG): „… für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind."

[88] *S. Ernst*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 4 DSGVO Rn. 95 f.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

(1) Jederzeitige Verfügbarkeit von Daten

Der Staat muss gewährleisten, dass solche Daten, die zur Erfüllung seiner Aufgaben notwendig sind, stets auch verfügbar sind.[89] Unter den Bedingungen moderner Informationsverarbeitung führt ein auch nur temporärer Datenverlust regelmäßig zu einem umfangreichen Ausfall von Verwaltungskapazitäten und hat ähnliche Effekte wie etwa ein Stromausfall. Ein solches Risiko kann sich in zweierlei Hinsicht realisieren: Zum einen besteht die Gefahr einer vorübergehenden Unverfügbarkeit von Daten, wenn diese in einen anderen Herrschaftsbereich ausgelagert werden und die Daten nicht zugleich in einer weiteren Version im eigenem Herrschaftsbereich verbleiben. Die vorübergehende Unverfügbarkeit von Daten kann dabei durch vielfältige technische Probleme eintreten. Zum anderen kann es zu einem dauerhaften Verlust von Daten kommen, etwa durch ein unbeabsichtigtes Löschen. Der dauerhafte Verlust kann sich auch aus einer vorübergehenden Unverfügbarkeit entwickeln, wenn die Daten zwar zukünftig wieder verfügbar sein werden, sich die Aufgabe, zu deren Zweck die Daten erforderlich waren, aber (aufgrund des Datenverlusts) erledigt hat. Die jederzeitige Datenverfügbarkeit zielt damit auch auf die Belastbarkeit von IT-Systemen und Diensten ab.[90]

Schließlich muss auch gewährleistet sein, dass ein Träger staatlicher Gewalt bei ordnungsgemäßer Beendigung eines Vertragsverhältnisses ohne Verzögerung die vollständige Verfügungsmacht über die Daten erhält und auch während einer Geschäftsbeziehung zu jeder Zeit eine vollumfängliche Verfügungsmacht in Anspruch nehmen kann. Dies entspricht der staatlichen Ausfallverantwortung mit jederzeitiger Rückholoption.

(2) Keine (inhaltliche) Verfälschung von Daten

Ebenso wichtig wie die Verfügbarkeit von Daten ist für die alltägliche Wahrnehmung öffentlicher Aufgaben durch Träger staatlicher Gewalt die inhaltliche Integrität der verwendeten Daten. Gerade beginnt sich etwa die staatliche Verwaltung verstärkt im Bereich der Massenverwaltung wie der Steuer- oder Sozialverwaltung unter Verweis auf die § 155 Abs. 4 AO, § 31a SGB X Entscheidungsprozessen zu öffnen, die vollständig automatisiert auf Grundlage einer Vielzahl von Daten ablaufen.[91] Aber nicht nur in solchen Konstellationen, sondern generell sind Daten in digitaler Form mittlerweile ein elementarer Faktor für die staatliche Verwaltungstätigkeit geworden. Ihre inhaltliche Richtigkeit kann sich unmittelbar auf die materielle Rechtmäßigkeit staatlicher Entscheidungen auswirken. Die inhaltliche

[89] Vgl. *Ernestus*, in: Simitis (Hrsg.), BDSG, § 9 Rn. 156 ff.; *Kramer/Meints*, in: Auernhammer, DSGVO/BDSG, Art. 32 DSGVO Rn. 31; *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 32 Rn. 27.

[90] Vgl. *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 32 Rn. 26.

[91] Vgl. dazu *Bull*, DVBl. 2017, 409; *Braun Binder*, DÖV 2016, 891; *Siegel*, DVBl. 2017, 24; *Stegmüller*, NVwZ 2018, 353.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Integrität solcher Daten, die für die Wahrnehmung öffentlicher Aufgaben relevant sind, hat deshalb eine besondere Bedeutung für die Richtigkeit von Verwaltungsentscheidungen.

Das Risiko inhaltlicher Verfälschung besteht dabei insbesondere deshalb, weil die inhaltliche Richtigkeit – anders als die Verfügbarkeit von Daten – für den einzelnen Amtswalter, der auf Grundlage der Daten handelt, nicht ohne weiteres erkennbar ist. Die Komplexität digitaler Datenbestände überfordert typischerweise die menschliche Wahrnehmung.[92] Eine inhaltliche Verfälschung von Daten kann deshalb dazu führen, dass über einen längeren Zeitraum unzutreffende Ergebnisse produziert werden. Aufgrund dieser weitreichenden Bedeutung ist die inhaltliche Integrität der fraglichen Daten unbedingt zu gewährleisten.

(3) Keine sachfremde Nutzung von Daten

Daten werden durch Träger staatlicher Gewalt stets zu einem bestimmten Zweck erhoben, gespeichert und genutzt. Bei diesem Grundsatz der Zweckbindung,[93] der sich etwa aus Art. 5 Abs. 1 lit. b DSGVO ergibt, handelt es sich um ein fundamentales Element zum Schutz Betroffener und zur Beschränkung staatlicher Befugnisse.

Grundsätzlich wird die staatliche Datenerhebung durch einen bestimmten Zweck gerechtfertigt. Die Datenweitergabe an weitere Akteure kann das Risiko einer sachfremden Nutzung steigern, wenn diese eigene Ziele verfolgen. So kann etwa schon ein abweichendes Interesse Dritter darauf gerichtet sein, ihnen überlassene Daten und das damit zusammenhängende Nutzungsverhalten auszuwerten, um die

[92] Nach der früheren DIN 44300 Nr. 19 waren Daten Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen. Bei Daten handelt es sich nach einem verbreiteten Verständnis um Zeichen oder kontinuierliche Funktionen, die im Gegensatz zu Information nicht frei interpretierbar, sondern nach festen Regeln formalisiert und reproduzierbar sind, *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, § 20 Rn. 11. Im Rahmen des Datenschutzrechts wird darauf hingewiesen, dass es für Daten notwendig sein soll, dass diese auf einem Datenträger verkörpert und dadurch wahrnehmbar sind und allein die Möglichkeit einer bloß sinnlichen Wahrnehmung und geistigen Aufnahme nicht ausreichend ist, *Eßer*, in: Auernhammer, DSGVO/BDSG, Art. 4 DSGVO Rn. 8. Bei digital verfassten Daten ist es durch die Codierung sogar der Normalfall, dass Daten und ihre Bedeutung nicht unmittelbar menschlich wahrnehmbar sind. Im Gegensatz dazu können Informationen als von einem Empfänger aufnehmbarer Sachverhalt verstanden werden, der geeignet ist, den Zustand oder das Verhalten des Empfängers zu beeinflussen, vgl. *Steinmüller u. a.*, in: BT-Drs. 6/3826, S. 5 (43); *Schoch*, VVDStRL 57 (1998), 158 (166); *ders.*, IFG, § 2 Rn. 16; *Reinhardt*, Wissen und Wissenszurechnung im öffentlichen Recht, S. 30; vgl. auch die Vorschrift des § 13 Abs. 1 S. 1 WpHG. Informationen bilden sich typischerweise aus Daten, sobald deren Aussagegehalt wahrnehmbar ist.

[93] Vgl. BVerfGE 65, 1 (46); *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 5 Rn. 63 ff.; *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 5 DSGVO Rn. 23 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

eigenen Systeme zu trainieren und zukünftige Technologien zu entwickeln. Es hat sich zu einem Grundprinzip der Datenökonomie entwickelt, dass vorhandene Daten auch genutzt werden. Auch wäre zu berücksichtigen, ob private IT-Dienstleister eigenständige, wie auch immer geartete Rechtspositionen an Daten, die ihnen übertragen werden, erlangen können.

Auch wenn sich solche Unterfangen auf personenbezogene Daten in anonymisierter oder pseudonymisierter Form beziehen, besteht die Gefahr, dass sich in Kombination mit anderen Daten eine Zuordnung zu einer bestimmten Person erreichen lässt und weitreichende Konsequenzen eintreten. Um solche oder sonstige sachfremde Nutzungen zu verhindern, muss deshalb auch sichergestellt werden, dass Daten, die den öffentlichen Herrschaftsbereich verlassen haben, nach der Erledigung ihres Verwendungszwecks unwiederbringlich gelöscht werden.

(4) Keine unbefugte Veröffentlichung von Daten

Schließlich ist sicherzustellen, dass Daten aus dem staatlichen Herrschaftsbereich nicht unbefugt veröffentlicht und allgemein zugänglich gemacht werden. Dieses Risiko der unbefugten Veröffentlichung betrifft verstärkt zum einen personenbezogene Daten der Bürger, die unter Verweis auf genuin staatliche Befugnisse erhoben worden sind und später für jedermann zugänglich werden. Zum anderen geraten diejenigen Daten in den Fokus, die Kernbereiche staatlicher Tätigkeit betreffen und etwa wesentliche interne Informationen einzelner Verfassungsorgane enthalten oder nationale Sicherheitsbelange betreffen.

Dieses Risiko betrifft nicht nur die Veröffentlichung solcher Daten, die unmittelbarer Gegenstand einer Verwaltungsaufgabe sind, sondern kann sich auch auf Daten erstrecken, die für die Verwaltung Arbeitsmittel sind. Mittlerweile wird ein Großteil gewöhnlicher Steuerbescheide durch die Steuerverwaltung vollständig automatisiert erlassen. Zur Kontrolle der vollständig automatisiert erlassenen Bescheide werden sog. Risikomanagementsysteme gemäß § 88 Abs. 5 AO eingesetzt, die – ebenfalls vollständig automatisiert – anhand verschiedener Kriterien mit Hilfe von Algorithmen bewerten, ob die vom Steuerpflichtigen gemachten Angaben plausibel sind. Nach § 88 Abs. 5 S. 4 AO dürfen Einzelheiten hierzu grundsätzlich nicht veröffentlicht werden, weil es die Gleichmäßigkeit und Gesetzmäßigkeit der Besteuerung gefährden könnte. Schon jetzt ist zu befürchten, dass Steuererklärungen dergestalt abgefasst werden, dass bekannte oder vermutete Kriterien der Risikomanagementsysteme ausgenutzt werden, um innerhalb eines Plausibilitätskorridors bewusst Angaben zu optimieren. Eine Veröffentlichung der Funktionsweise dieser Risikomanagementsysteme würde deshalb die Tätigkeit der Steuerverwaltung in einem weiten Bereich untergraben.

Auch im Hinblick auf die Gefahr einer unbefugten Veröffentlichung von Daten ist deshalb sicherzustellen, dass die Daten zu löschen sind, sobald sich ihr Bedarf er-

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

ledigt hat. Solange Daten vorhanden sind, erhöht jede Kopie und jeder weitere Speicherort das Risiko einer Weiterverbreitung.

bb) Wesensmerkmale von Daten

Für die nähere Ausgestaltung einer Gewährleistungsverantwortung als Reaktion auf diese Risiken sind die Wesensmerkmale von Daten und die Besonderheiten des Umgangs mit ihnen zu berücksichtigen.

Die tatsächlichen Bedingungen, unter denen Daten im Alltag übertragen werden können, weichen elementar von der Struktur ab, die für gewöhnliche Sachen und Rechte besteht. Daten und Informationen weisen einen nicht-rivalen Charakter auf, weil die Nutzung durch eine Person nicht die Nutzung durch eine andere Person ausschließt.[94] In Verbindung mit der ubiquitären, kostengeringen und effektiven Möglichkeit der digitalen Kopie[95] führt dies etwa dazu, dass das Risiko einer unbefugten Veröffentlichung steigt – unerheblich ob beabsichtigt oder nicht. Da sich Daten schnell, ohne nennenswerten Aufwand und mit geringen Kosten übertragen lassen, nimmt mit jeder weiteren Datenübertragung und jeder zusätzlichen Zugriffsmöglichkeit die Gefahr zu, dass die betreffenden Daten den Weg in die Öffentlichkeit finden. Unter den Bedingungen moderner Informationstechnologien lässt sich sogar konstatieren, dass sich bereits mit der erstmaligen Weitergabe von Daten die Tendenz einer weiteren Streuung ergibt, solange nur ein ausreichend starkes tatsächliches Interesse am Inhalt der Daten besteht.[96] Eine einmal vorgenommene Verbreitung oder gar Veröffentlichung von Daten sowie der darin enthaltenen Informationen lässt sich deshalb faktisch kaum mehr rückgängig machen.[97]

---

[94] *Schoch*, IFG, § 2 Rn. 16; *Druey*, Information als Gegenstand des Rechts, S. 33; *Mayer-Schönberger*, SJZ 97 (2001), 383 (384); *Spinner*, in: Schweizer/Burkert/Gasser (Hrsg.), FS Druey, S. 947 (958); *Ott*, Information, S. 41. Vgl. auch *Mayer-Schönberger*, in: Schweizer/Burkert/Gasser (Hrsg.), FS Druey, S. 853 (860); *Püschel*, Informationen des Staates als Wirtschaftsgut, S. 41.

[95] *Picot*, in: Kubicek/Klumpp/Müller u. a. (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1997, S. 42 (56); *Stransfeld*, in: Tauss/Kollbeck/Mönikes (Hrsg.), Deutschlands Weg in die Informationsgesellschaft, S. 684 (684 f.); *Mayer-Schönberger*, in: Schweizer/Burkert/Gasser (Hrsg.), FS Druey, S. 853 (860); *Püschel*, Informationen des Staates als Wirtschaftsgut, S. 41.

[96] *Picot*, in: Kubicek/Klumpp/Müller u. a. (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1997, S. 42 (56). Vgl. *Egloff*, DVR 7 (1978), 115 (116 ff.).

[97] Mit einem Schwerpunkt auf dem Element Information VGH Mannheim NVwZ 2011, 443 (444); OVG Greifswald ZUR 2009, 375 (376); VG Wiesbaden MMR 2009, 428 (430 f.); *Hoffmann-Riem*, AöR 134 (2009), 513 (524); *Schoch*, NJW 2012, 2844 (2845); *ders.*, NJW 2010, 2241 (2242); *ders.*, in: Isensee/P. Kirchhof (Hrsg.), HStR III, § 37 Rn. 107; *Ossenbühl*, NVwZ 2011, 1357 (1358); f. *Becker/Blackstein*, NJW 2011, 490 (490); *Wollenschläger*, VerwArch 102 (2011), 20 (43 f.); *Heintzen*, NuR 1991, 301 (303); *Tinnefeld*, RDV 2009, 47 (50); *Hornung*, MMR 2004, 3 (5); *Käß*, WiVerw 2002, 197 (208); *Fischer/Fluck*, NVwZ 2013, 337 (339); *Krause*, Rechtsformen des Verwaltungshandelns, S. 331. Vgl. BGHZ 31, 308 (314 f.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Berücksichtigt man weiter, dass Daten außerdem so dargestellt werden können, dass sie menschlich wahrnehmbar sind (und damit Informationen bilden), kommt hinzu, dass schon diese menschliche Wahrnehmung und Rezeption für eine Weiterverbreitung ausreicht. Auch dies steht der Rückgängigmachung einer einmal vorgenommenen Veröffentlichung im Wege. Selbst wenn eine bestimmte Person als rechtmäßiger Inhaber von Daten angesehen werden könnte, kann, sobald es um den wahrgenommenen Informationsgehalt geht, diese Person auf andere Rezipienten nicht derart einwirken, dass sie die fragliche Information wieder vergessen. Rechtlich wäre in solchen Situationen im Übrigen auch die Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG zu berücksichtigen, denn auch eine rechtswidrig erlangte und rechtswidrig veröffentlichte Information ist allgemein zugänglich i.S.d. Art. 5 Abs. 1 S. 1 GG und ihre Wahrnehmung unterfällt dem grundrechtlichen Schutzbereich.[98] Selbst bei einer unrechtmäßigen Verbreitung von Daten und den darin enthaltenen Informationen in Form einer Veröffentlichung ist es also praktisch kaum möglich, diesen Vorgang rückgängig zu machen.

Auch für einen dauerhaften Datenverlust liegt es in der Natur der Sache, dass sich dies faktisch nicht wieder rückgängig machen lässt. Die Möglichkeit, eine sachfremde Nutzung rückgängig zu machen, hängt von dem Effekt der Nutzung ab. Die Nutzung an sich lässt sich nicht rückgängig machen, möglicherweise kann aber deren Konsequenz rückgängig gemacht werden. So könnte z. B. theoretisch der Ertrag einer sachfremden Nutzung abgeschöpft werden, auch wenn dafür praktisch verschiedene (auch rechtliche) Hürden bestehen dürften. Die inhaltliche Verfälschung von Daten lässt sich am unproblematischsten wieder beheben, allerdings setzt dies voraus, dass ein weiterer korrekter Datensatz existiert. Da dieser permanent gepflegt und aktuell gehalten werden müsste, ginge dies mit einem erheblichen Mehraufwand einher.

Für die Umsetzung der mit der Gewährleistungsverantwortung verbundenen Rückholoption im Falle privater Schlechterfüllung (Ausfallverantwortung) im Bereich der Datenverarbeitung verlangen diese Wesensmerkmale von Daten deshalb nach einem Paradigmenwechsel. Im Gegensatz zu anderen staatlichen Aufgaben sind hier Konstellationen möglich, in denen zwar die abstrakte (Datenverarbeitungs-) Aufgabe durch den Staat wieder zurückgeholt werden kann, eine konkrete (Nach-) Erfüllung aber nicht mehr möglich ist. Beim Umgang mit Daten sind strukturbedingt negative Folgen denkbar, die sich unumkehrbar in die Zukunft erstrecken. Während also bei anderen staatlichen Aufgaben die Kontrolle zumindest ex-nunc wiedererlangt, geschehene Fehler korrigiert und ein ordnungsgemäßer Zustand wiederhergestellt werden kann, kann im Hinblick auf Daten zwar die Aufgabenwahrnehmung wieder übernommen werden, die aus dem geschehenen Fehler resultierenden Konsequenzen für Daten können aber häufig nicht mehr rückgängig gemacht werden, so dass der entstandene unerwünschte Zustand schlicht als unumkehrbar ak-

[98] *Degenhart*, in: Bonner Kommentar, GG, Art. 5 I, II Rn. 304; *Starck/Paulus*, in: v. Mangoldt/Klein/Starck, GG, Art. 5 Rn. 116; *Dörr*, in: Merten/Papier (Hrsg.), HGR IV, § 103 Rn. 35 f; *Schulze-Fielitz*, in: Dreier (Hrsg.), GG, Art. 5 I, II Rn. 82.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

zeptiert werden muss. Dies kann z. B. daran liegen, dass die dafür notwendigen Daten irreversibel verloren sind oder die exklusive öffentlich-rechtliche Inhaberschaft über bestimmte Daten durch eine Veröffentlichung unwiederbringlich aufgehoben worden ist. Mögliche negative Folgen bei der Wahrnehmung sonstiger staatlicher Aufgaben beschränken sich hingegen typischerweise auf das Ereignis, das die Auffangverantwortung ausgelöst hat, weisen aber keine vergleichbaren dauerhaften Konsequenzen auf. Aufgrund der Natur von Daten lässt sich deshalb schwerlich davon sprechen, dass sich die staatliche Gewährleistungsverantwortung bei der Einbindung privater IT-Dienstleister stets durch eine effektive Rückholoption absichern ließe.

Zwar kann man Daten eine Unterstützungsfunktion für die staatliche Verwaltung zusprechen, die vergleichbar auch für eine Vielzahl anderer Tätigkeiten oder Gegenstände besteht, die in private Hände gegeben sind, wie etwa der Straßenunterhalt oder ein Fahrzeugpark. Dass in solchen Fällen die Einbeziehung Privater regelmäßig unproblematisch ist, beim Umgang mit Daten aber erhebliche Schwierigkeiten aufweist, ist auf die besonderen Wesensmerkmale von Daten zurückzuführen. In den gewöhnlichen Fällen der Einbindung Privater stehen für den Fall, dass diese nicht mehr in der Lage sind, ihre Tätigkeiten fortzuführen, grundsätzlich Ersatzakteure auf dem Markt zur Verfügung, die an die Stelle des bisherigen privaten Dienstleisters treten können. Beim Umgang mit Daten geht es aber nicht nur darum, einen Ersatzdienstleister ausfindig zu machen, was selbst bei besonderen technischen Standards grundsätzlich möglich sein dürfte. Zusätzlich bedarf es auch der Daten in ihrem ursprünglichen Zustand und dies kann unmöglich geworden sein.

b) Allgemeine Geschäftsrisiken im Lichte des IT-Outsourcings und der Datenübermittlung in einen privaten Hoheitsbereich

Bei der Einbindung Privater in die Wahrnehmung öffentlicher Aufgaben können, abseits der beschriebenen IT-spezifischen Gefahren, eine Vielzahl allgemeiner Geschäftsrisiken bestehen. Diese können sich vor dem Hintergrund der beschriebenen tatsächlichen Rahmenbedingungen beim IT-Outsourcing und bei der Datenübermittlung in einen privaten Hoheitsbereich besonders gravierend auswirken.

aa) Individuelle fachliche Qualifikation, Informations- und Machtasymmetrien[99]

Die Einbindung privater IT-Dienstleister in die Wahrnehmung öffentlicher Aufgaben erfordert die Spezifizierung der Leistungen, die vom Privaten erwartet

[99] Auch wenn die folgenden Ausführungen schon auf den IT-Sektor zugeschnitten sind, handelt es sich bei dem Problem individueller fachlicher Qualifikation und Informationsasymmetrien um ein Risiko, das nicht alleine im IT-Sektor besteht, sondern ein allgemeines Risiko darstellt, das auch in vielen anderen Bereichen auftauchen kann.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

werden. In aller Regel erfolgt dies im Rahmen von Vertragsverhandlungen zwischen dem Träger staatlicher Gewalt und dem privaten IT-Dienstleister.[100] Eine besondere Bedeutung kommt deshalb den Vertragsmerkmalen zu, welche die Einbindung privater IT-Dienstleister in die staatliche Aufgabenwahrnehmung betreffen.[101] Das macht es notwendig, dass hinreichend qualifiziertes Fachpersonal auch beim Träger staatlicher Gewalt vorhanden sein muss. Dieses muss die geforderten Leistungen in technischer Hinsicht genau spezifizieren können und muss sich darüber im Klaren sein, was technisch möglich ist und verlangt werden kann, insbesondere für den Fall einer mangelhaften Leistungserbringung durch den privaten IT-Dienstleister. Trotz der immer spezieller werdenden Ausbildung und steigenden personellen Ausstattung von IT-Abteilungen bei Trägern staatlicher Gewalt dürfte nach wie vor ein Mangel an IT-Fachkräften bestehen. Die notwendigen IT-Fähigkeiten und Kenntnisse können deshalb auf Seiten der Träger staatlicher Gewalt nicht pauschal vorausgesetzt werden. Erschwert wird die Situation zudem dadurch, dass diese Fähigkeiten und Kenntnisse bei jeder öffentlichen Stelle vorhanden sein müssten, die selbständig private IT-Dienstleister in Anspruch nimmt, im Zweifel also etwa auch bei Kommunen.[102]

Einer Begegnung auf Augenhöhe zwischen Trägern staatlicher Gewalt und privaten IT-Dienstleistern steht in der Praxis typischerweise ein weiteres Hindernis entgegen. Insbesondere große IT-Dienstleister bieten häufig vorgefertigte Leistungspakete an, doch diese Standardverträge berücksichtigen selten ausreichend die konkreten Bedürfnisse des Kunden und sind regelmäßig zugunsten des privaten IT-Dienstleisters ausgestaltet.[103] Ein individuelles Abweichen erfordert nicht nur detaillierte fachliche Kenntnisse, auch gerade über das, was dem privaten IT-Dienstleister technisch möglich sowie angesichts des Vertragsgegenstands und -volumens zumutbar ist und deshalb von ihm verlangt werden kann. Hier besteht in aller Regel eine erhebliche Informationsasymmetrie zugunsten des privaten IT-Dienstleisters.[104] Die Möglichkeit einer individuellen Vertragslösung muss darüber hinaus auch die Marktmacht des Anbieters berücksichtigen und in dieser Hinsicht haben sich einzelne private IT-Dienstleister mittlerweile eine herausragende Stellung erarbeitet.

Aufgrund ihrer (legitimen) privatnützigen Ausrichtung bedienen sich private IT-Dienstleister dieser Effekte und forcieren sie typischerweise zur eigenen Gewinnmaximierung. Im Gegensatz dazu sind IT-Dienstleistungen, die in einem hoheitlich geprägten Einflussbereich erbracht werden, an einheitliche gesetzliche Regelwerke gebunden, auf Gemeinwohlziele ausgerichtet und von Amtspflichten geprägt.

---

[100] Vgl. allgemein *Gründer*, DuD 2016, 667; *Debski*, DuD 2016, 659; *v. Faber*, DuD 2016, 647.

[101] *Griesser/Buntschu*, DuD 2016, 640 (641).

[102] *Schulz*, DuD 2015, 466 (467, 469).

[103] *Griesser/Buntschu*, DuD 2016, 640 (646).

[104] *Gründer*, DuD 2016, 667 (667); vgl. auch *Schulz*, DuD 2016, 466 (469); *Martini*, Digitalisierung als Herausforderung und Chance für Staat und Verwaltung, S. 14 f.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

bb) Unabhängigkeit und Unzugänglichkeit von privaten IT-Dienstleistern

In einem engen Zusammenhang mit den beschriebenen Informations- und Machtasymmetrien steht eine gesteigerte Unabhängigkeit und Unzugänglichkeit privater IT-Dienstleister. Nach Art. 28 Abs. 3 lit. h DSGVO müssen – private wie öffentliche – Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der ihnen obliegenden Pflichten zur Verfügung stellen und Überprüfungen einschließlich Inspektionen ermöglichen. Die tatsächliche Umsetzung dieser Kontrollrechte muss jedoch die Auswirkungen der allgemeinen Geschäftsrisiken berücksichtigen, die gerade im IT-Bereich zu einer weitgehenden Abkapselung privater IT-Dienstleister führen können. Diese beruht im Einzelnen auf einer erheblich gesteigerten Marktmacht, einem typischerweise bestehenden fachlichen Informationsvorsprung sowie der rechtlichen Selbständigkeit.

Aufgrund dieser Umstände können sich Risiken durch fehlende Prüf- und Aufsichtsrechte des eigentlichen Dateninhabers ergeben. Als Folge von Informationsasymmetrien werden gerade Sicherheitsfragen häufig schon bei der Anbahnung von Geschäftsverbindungen mit IT-Dienstleistern nicht ausreichend berücksichtigt.[105] Insbesondere das operationelle Vorgehen auf Mitarbeiterebene und die Betriebsabläufe sind typischerweise für den ursprünglichen Dateninhaber nicht zugänglich, beeinflussbar oder gar durch Weisungsrechte steuerbar.[106] Dies gilt umso mehr, wenn durch den IT-Dienstleister weitere nachgelagerte Unternehmer einbezogen werden oder wesentliche Betriebsabläufe im Ausland stattfinden. Die Ausgestaltung dieser internen Abläufe ist aber von essenzieller Bedeutung für die Wahrscheinlichkeit, dass sich die beschriebenen Gefahren beim Verarbeiten von Daten realisieren.

Diese Probleme setzen sich auf der Ebene der IT-Systeme fort. Insbesondere Private verfolgen regelmäßig ein proprietäres Geschäftsmodell, was dazu führt, dass Dritte keinen Einblick in die konkrete Struktur und Technik der eingesetzten IT-Systeme haben. Der Ausübung von Kontrollrechten können grundrechtlich geschützte Geschäfts- und Betriebsgeheimnisse entgegengehalten werden. Das Implementieren neuer Funktionen, das Wissen um die Aufschlüsselung von Kosten und das Schließen etwaiger Sicherheitslücken ist regelmäßig alleine dem IT-Dienstleister möglich.[107] Damit steigt das Risiko eines Verlusts der Kontroll- und Steuerungsfähigkeit, vor allem im Hinblick auf die jederzeitige Verfügbarkeit und inhaltliche Integrität von Daten und damit die Funktionsfähigkeit der Verwaltung insgesamt.

Hinzu kommt, dass sich auf dynamischen Märkten, zu denen insbesondere der IT-Sektor gehört, sog. Netzeffekte bilden.[108] Im dynamischen Markt ist der Nutzen einer

[105] Vgl. *Schmelling*, DuD 2016, 635 (638).

[106] *Griesser/Buntschu*, DuD 2016, 640 (645); vgl. *Debski*, DuD 2016, 659 (665).

[107] Vgl. *Heckmann/Bernhardt*, Digitale Gewaltenteilung als Marktverantwortung, S. 11.

[108] Neben dem Begriff „Netzeffekte" finden sich auch die Bezeichnungen „Netzwerkeffekte" und „Netzwerkexternalitäten", vgl. dazu *Zimmerlich*, Marktmacht in dynamischen Märkten, S. 78; *Stopper*, ZWeR 2005, 87 (96).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Ware oder Dienstleistung umso höher, je mehr Nutzer existieren.[109] Neben einem direkten Netzeffekt, der unmittelbar mit der Anzahl weiterer Nutzer zusammenhängt, kann auch ein indirekter Netzeffekt beobachtet werden, der den Nutzen einer Ware oder Dienstleistung umso mehr steigert, je mehr komplementäre Güter verfügbar sind und je mehr Nutzer mit dem Umgang des Guts (bzw. der Technologie) vertraut sind, etwa einem konkreten Betriebssystem.[110] Dahinter steht vor allem im IT-Sektor das Setzen einheitlicher Standards. Für die staatliche Verwaltung stellt dies ein besonderes Risiko dar, weil die einzelnen Träger staatlicher Gewalt auf einen Datenaustausch untereinander angewiesen sind. Sollten dem aber technische Hürden entgegenstehen, etwa durch uneinheitliche Standards, wäre die Funktionsfähigkeit der Verwaltung insgesamt in Frage gestellt.

Sobald sich ein bestimmter Standard durchsetzt, entfaltet dies durch die Zunahme komplementärer Güter und sich verstärkender Netzeffekte eine Sogwirkung, die zur Machtkonzentration im Markt führt.[111] Die Nutzer bestimmter Systemstandards neigen dazu, diese Systeme nicht zu verlassen, weil ansonsten hohe Wechselkosten entstehen könnten. Investitionen in komplementäre Güter würden bei einem Verlassen des Standards verloren gehen und gleichzeitig wären neue Investitionen notwendig. Private IT-Dienstleister nutzen diesen sog. Lock-in-Effekt teilweise bewusst zur Bindung ihrer Kunden aus.[112] Damit entsteht ein Kreislauf, der die Abhängigkeit von IT-Dienstleistern stetig intensiviert.

cc) Insolvenzrisiko

Für IT-Dienstleister kann sich Kostendruck als ein wesentlicher Betriebsfaktor erweisen. Dabei steht die jederzeitige Verfügbarkeit von Daten unter dem Vorbehalt, dass der Betrieb der IT-Systeme gesichert ist. Aber auch das Sicherheitsniveau, die personelle Ausstattung und die Qualität der Fachkräfte kann durch die Finanzkraft eines IT-Dienstleisters beeinflusst werden.

Bei privaten IT-Dienstleistern besteht neben dem allgemeinen Risiko eines zu geringen Finanzeinsatzes auch ein Insolvenzrisiko,[113] unabhängig von der konkret gewählten privatrechtlichen Rechtsform. Eine insolvenzbedingte Einstellung des Geschäftsbetriebs kann spontan und ohne Vorwarnung eintreten und zumindest zu einer nicht unerheblichen vorübergehenden Unverfügbarkeit von Datenbeständen führen. Zwar bestimmt Art. 32 Abs. 1 lit. c DSGVO, dass auch Private im Rahmen

[109] *Gey*, WuW 2001, 933 (934); *Fleischer/Körber*, K&R 2001, 623 (624); *Fichert/Sohns*, WuW 2004, 907 (911); *Stopper*, ZWeR 2005, 87 (96 f.); *Zimmerlich*, WRP 2004, 1260 (1261).

[110] *Zimmerlich*, Marktmacht in dynamischen Märkten, S. 79 ff.; *dies.*, WRP 2004, 1260 (1261); *Dreher*, ZWeR 2009, 149 (152 f.); *Stopper*, ZWeR 2005, 87 (96 f.); *Fichert/Sohns*, WuW 2004, 907 (911 f.).

[111] *Zimmerlich*, Marktmacht in dynamischen Märkten, S. 88; *dies.*, WRP 2004, 1260 (1262 f.).

[112] Vgl. *Griesser/Buntschu*, DuD 2016, 640 (644).

[113] *Griesser/Buntschu*, DuD 2016, 640 (644).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

der Auftragsverarbeitung ein angemessenes Schutzniveau sicherstellen müssen, wozu auch die Fähigkeit gehört, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen technischen Zwischenfall rasch wiederherzustellen. Dabei ist aber schon fraglich, ob etwa eine Insolvenz als physischer technischer Zwischenfall einzuordnen wäre und ob in einem solchen Fall nicht ohnehin rechtliche Verpflichtungen an ihre faktischen Grenzen stoßen. Auch zielt die Regelung direkt nur auf personenbezogene Daten ab, nicht aber auf die Verarbeitung anderer Daten, die ebenfalls eine essenzielle Bedeutung für die Verwaltung haben können. Konkrete Angaben zum Mindestmaß, das von Privaten sichergestellt werden muss, lassen sich der Vorschrift schließlich auch nicht entnehmen.

dd) Individuelles Fehlverhalten

Für die Annahme eines besonderen Risikos bei einem privaten Zugriff auf staatlich erhobene Daten kann nicht auf die pauschale Befürchtung eines rechtswidrigen Verhaltens durch Private abgestellt werden. Ohne weitere konkrete Umstände lässt sich Individuen, die privat tätig werden, ein rechtswidriges Verhalten ebenso wenig unterstellen wie denjenigen, die öffentliche Aufgaben wahrnehmen. Anders gewendet besteht ein solches Risiko grundsätzlich immer dort, wo Menschen in Arbeitsprozesse eingebunden sind.[114]

Entscheidend für das spezifische Risiko eines individuellen Fehlverhaltens Privater sind vielmehr die strukturellen Unterschiede auf einer normativen Ebene, die zwischen öffentlich-rechtlichem und privatrechtlichem Handeln bestehen. Nach der Rechtsprechung des Bundesverfassungsgerichts ist insofern zu berücksichtigen, dass bei privatem Tätigwerden spezifische, gesetzlich konkretisierte Amtspflichten fehlen und das Handeln stattdessen privatnütziger Natur ist.[115] Auch der Europäische Gerichtshof weist darauf hin, dass bei der Verarbeitung personenbezogener Daten durch Private ausreichende rechtliche Garantien vorhanden sein müssen, die einen wirksamen Schutz gegen Missbrauch, unberechtigten Zugang zu den Daten und ihre unberechtigte Nutzung ermöglichen.[116] Zur Sicherstellung solcher Vorgaben bieten sich in der Praxis verschiedene Mittel an. So kann das Vier-Augen-Prinzip für den Zugriff auf Daten vorgeschrieben werden oder der Zugriff auf Daten revisionssicher protokolliert werden.[117]

Nach Art. 28 Abs. 3 lit. b DSGVO müssen zwar auch Private im Rahmen einer Auftragsverarbeitung gewährleisten, dass die zur Datenverarbeitung befugten Personen sich zumindest zur Vertraulichkeit verpflichtet haben. Dabei ist aber zweifelhaft, ob privatrechtliche Verpflichtungen dasselbe Schutzniveau erreichen wie öffentlich-rechtliche Amtspflichten. Außerdem betrifft die Regelung des Art. 28

[114] *Debski*, DuD 2016, 659 (665).

[115] BVerfGE 125, 260, Rn. 222.

[116] EuGH, Urt. v. 6. 10. 2015, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650, Rn. 91.

[117] BVerfGE 125, 260, Rn. 222.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Abs. 3 lit. b DSGVO ausdrücklich nur die Personen, die zur „Datenverarbeitung" befugt sind, nicht aber andere Personen, die lediglich faktisch auf die Daten zugreifen können.

Diese Unterschiede im Schutzniveau bestehen auch auf strafrechtlicher Ebene, weil es möglich ist, dass Mitarbeiter privater IT-Dienstleister nicht denselben Strafandrohungen ausgesetzt sind wie Amtsträger.[118] Relevant ist hier in erster Linie die Verletzung von Privatgeheimnissen nach § 203 StGB. Die Berufsgruppe der Mitarbeiter privater IT-Dienstleister werden in § 203 Abs. 1 StGB nicht als taugliche Täter genannt. Amtsträger i.S.d. § 11 StGB sind hingegen über § 203 Abs. 2 S. 1 Nr. 1 StGB erfasst. Hierzu gehören nach § 11 Abs. 1 Nr. 2 c) StGB auch diejenigen Personen, die dazu bestellt sind, bei einer Behörde oder bei einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung unbeschadet der zur Aufgabenerfüllung gewählten Organisationsform wahrzunehmen. Auch diejenigen, die keine Amtsträger sind, wohl aber für den öffentlichen Dienst besonders Verpflichtete (§ 11 Abs. 1 Nr. 4 StGB), sind taugliche Täter des § 203 StGB. § 30 Abs. 9 AO verlangt diese Qualifizierung ausdrücklich, damit im Rahmen einer Auftragsverarbeitung das Steuergeheimnis gewahrt bleibt. Ob Mitarbeiter von privaten IT-Dienstleistern als für den öffentlichen Dienst besonders Verpflichtete gemäß §§ 203 Abs. 2 S. 1 Nr. 2, 11 Abs. 1 Nr. 4 StGB angesehen werden können, kann von verschiedenen Faktoren abhängen und lässt sich nicht pauschal beurteilen, insbesondere weil es dazu einer förmlichen Verpflichtung der konkreten Mitarbeiter aufgrund eines Gesetzes bedürfte.[119]

Während die Strafbarkeit nach § 203 StGB vor allem Angehörige von Trägern öffentlicher Gewalt treffen dürfte, richtet sich die Strafvorschrift des § 42 BDSG an Amtsträger und für den öffentlichen Dienst besonders Verpflichtete sowie Mitarbeiter privater IT-Dienstleister gleichermaßen. Die dortige Strafandrohung und damit das Schutzniveau ist jedoch aufgrund der tatbestandlichen Grenzen nicht mit der des § 203 StGB vergleichbar. § 42 Abs. 1 BDSG erfasst die unberechtigte Datenübermittlung an Dritte oder das Zugänglichmachen auf andere Art und Weise, setzt aber voraus, dass dies wissentlich geschieht, nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen betrifft und gewerbsmäßig geschieht. Im Gegensatz zu § 203 StGB reicht das bloß unbefugte Offenbaren nicht aus. § 42 Abs. 2 BDSG betrifft daneben die unberechtigte Verarbeitung personenbezogener Daten oder ihr Erschleichen durch unrichtige Angaben, fordert aber weiter ein Handeln gegen Entgelt, in Bereicherungsabsicht oder Schädigungsabsicht. Zwar nicht pauschal, aber aufgrund normativ-struktureller Unterschiede kann mit der Einbindung Privater das Risiko eines individuellen Fehlverhaltens also steigen.

[118] Vgl. *Conrad/Strittmatter*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 22 Rn. 202.

[119] Vgl. *Eser/Hecker*, in: Schönke/Schröder, StGB, § 11 Rn. 33 ff.; *v. Heintschel-Heinegg*, in: ders. (Hrsg.), BeckOK StGB, § 11 Rn. 40 f.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

ee) Handeln und Einflüsse Dritter

Dritte, die außerhalb der Geschäftsbeziehung zwischen dem Träger staatlicher Gewalt und dem IT-Dienstleister stehen, können das Risiko, das mit einer Datenübertragung in einen privaten Hoheitsbereich verbunden ist, weiter steigern. Zu denken ist hier an Organe von Drittstaaten oder andere Private, die ebenfalls Angebote des IT-Dienstleisters in Anspruch nehmen. Insbesondere wenn in Anspruch genommene IT-Dienstleister dem Regelungsregime eines anderen Staates unterfallen, lässt sich kaum ausschließen, dass diese nach ihrem nationalstaatlichen Recht verpflichtet sind, insbesondere Sicherheitsbehörden Zugriff auf die bei ihnen vorhandenen Daten zu ermöglichen.[120]

Wenn die IT-Dienstleistung, auf die der Träger staatlicher Gewalt zugreift, parallel von (privaten) Dritten in Anspruch genommen werden kann, muss auch dies als Sicherheitsrisiko bewertet werden. Dritte, die ebenfalls Zugriff auf die IT-Dienstleistung haben, können damit schon erste Sicherheitsbarrieren überschreiten und so eine größere Chance auf einen missbräuchlichen Datenzugriff insgesamt erhalten.[121] Außerdem erscheint es denkbar, dass Dritte die IT-Dienstleistung zu einem gesonderten rechtswidrigem Handeln nutzen und dies auf die allgemeine Nutzung der IT-Dienstleitung nachteilig zurückfällt, weil etwa durch Maßnahmen von Ermittlungsbehörden die Inanspruchnahme der Dienstleistung insgesamt eingeschränkt wird.

Dritte können auch Zugriffsmöglichkeiten auf Daten, die bei einem privaten IT-Dienstleister vorhanden sind, auf rechtlich zulässigem Wege erhalten. So ist es denkbar, dass Dritte die Kontrolle über einen privaten IT-Dienstleister im Wege einer Unternehmensübernahme erlangen. Diese Möglichkeit steht auch gerade ausländischen Dritten offen.[122] Eine Change of Control-Klausel kann zwar zur Vertragsbeendigung und Löschpflichten führen, beendet aber auch die Aufgabenerfüllung. Schließlich kann sich eine Gefahr durch Rechtsstreitigkeiten des IT-Dienstleisters ergeben, die dieser mit Dritten führt. Zwar ist vereinzelt bestimmt, wie in § 497 Abs. 3 StPO, dass eine Pfändung von privaten Einrichtungen, die im Auftrag einer öffentlichen Stelle Daten verarbeiten, unzulässig ist. Wo dies aber nicht ausdrücklich bestimmt ist, können Einrichtungen eines IT-Dienstleisters gepfändet oder mit vergleichbaren dinglichen Rechten belastet werden. Dies könnte die Verfügbarkeit der Daten in Frage stellen sowie zu einer sachfremden Nutzung oder unbefugten Veröffentlichung führen.

[120] Vgl. *Emmert*, DuD 2016, 34. vgl. die sog. No Spy Erklärung des Bundesinnenministeriums vom 30. 4. 2014, Az. O4 – 11032/23#14.

[121] *Debski*, DuD 2016, 659 (665).

[122] Gegebenenfalls kann hier eine Prüfung nach § 60 Abs. 1 S. 1 Nr. 3 AWV notwendig werden.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

3. Konkretisierung der Gewährleistungsverantwortung

Diese Risiken im Zusammenhang mit IT-Dienstleistungen sind bei der Konkretisierung der staatlichen Gewährleistungsverantwortung sowie der Frage zu berücksichtigen, wie diese erfüllt werden kann. Außerhalb des engen Bereichs obligatorischer Staatsaufgaben lassen sich Aufgabenbereiche, bei denen Daten nicht in private Einflusssphären übermittelt werden dürfen, nicht generell und abschließend identifizieren. Dies ist vielmehr von den konkreten Einzelfallumständen und einer Abwägung abhängig und kann auch etwa den Inhalt betroffener Daten berücksichtigen. In dieser Hinsicht lässt sich zwischen einer Gewährleistungsverantwortung nach innen und nach außen unterscheiden.

a) Gewährleistungsverantwortung nach innen

Angesichts der Risiken bei der Einbindung privater IT-Dienstleister besteht eine staatliche Gewährleistungsverantwortung zunächst im Hinblick auf die Funktionsfähigkeit staatlicher Funktionen, namentlich die Wahrnehmung von Verwaltungsaufgaben. Dabei stellt sich die Frage, ob die staatliche Gewährleistungsverantwortung im Falle der Einbindung privater IT-Dienstleister in ausreichendem Maße wahrgenommen werden kann.

aa) Aufrechterhaltung und Absicherung von Verwaltungsfunktionen

Der Staat muss gewährleisten, dass seine Funktionsfähigkeit im Hinblick auf die Wahrnehmung von Verwaltungsaufgaben und die Erledigung von Verwaltungsvorgängen unangetastet bleibt. Dazu kann, je nach Bedeutung von konkretem Sachbereich und Dateninhalt, auch die Fähigkeit zum jederzeitigen Datenzugriff und der Verwendung nicht korrumpierter Daten gehören. Insofern muss die Summe der oben beschriebenen Risiken berücksichtigt werden. Zugleich müssen die teils gegenläufigen institutionellen Strukturen privater wie öffentlich-rechtlicher IT-Dienstleister sowie die sich daraus ergebenden Konsequenzen beachtet werden.

(1) Finanzielle Versorgung und Stabilität der Leistungserbringung

IT-Dienstleister in öffentlich-rechtlicher Rechtsform werden – anders als private IT-Dienstleister – nicht durch ein privatrechtliches Rechtsgeschäft, sondern einen Errichtungsakt des Staates gegründet. In Betracht kommt dafür eine Organisation als Anstalt des öffentlichen Rechts, die von einem oder mehreren Trägern öffentlicher Gewalt errichtet wird. Diese Träger haften im Rahmen der sog. Gewährträgerhaftung grundsätzlich gegenüber Dritten zwar subsidiär, aber unbeschränkt für die Verbindlichkeiten der Anstalt.[123] Daneben tritt die sog. Anstaltslast, aufgrund der die

[123] *Müller*, in: H. J. Wolff/Bachof/Stober/Kluth, Verwaltungsrecht II, § 86 Rn. 19.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Träger die Funktionsfähigkeit der Anstalt gewährleisten müssen, solange die Anstalt besteht; dazu gehört gegebenenfalls auch eine finanzielle Unterstützung.[124]

Bei der Gewährträgerhaftung und Anstaltslast handelt es sich nach der Rechtsprechung zwar nicht um verbindliche Rechtsnormen im eigentlichen Sinne.[125] Für öffentliche IT-Dienstleister werden deren Inhalte und Vorgaben aber, je nach Rechtsform, häufig ausdrücklich klargestellt. Veranschaulicht werden kann dies anhand von Dataport, dem IT-Dienstleister für verschiedene Landes- und Steuerverwaltungen sowie Kommunen, als Anstalt des öffentlichen Rechts. § 2 Abs. 5 des Dataport-Staatsvertrags stellt ausdrücklich klar, dass die Träger der Anstalt – verschiedene Bundesländer – für die auf der Anstalt lastenden Verbindlichkeiten unbeschränkt haften. Nach § 2 Abs. 6 des Dataport-Staatsvertrags stellen die Träger außerdem sicher, dass die Anstalt für die Dauer ihres Bestehens als Einrichtung funktionsfähig bleibt. Angesichts der Aufgabenbestimmung des § 3 Abs. 1 des Dataport-Staatsvertrags – die Unterstützung der öffentlichen Verwaltungen einschließlich der Kommunalverwaltungen in verschiedenen Bundesländern als (zentraler) IT-Dienstleister – wird schon damit effektiv eine Vielzahl der beschriebenen Risiken erheblich abgeschwächt. Hinzu kommt, dass es sich bei den Trägern um Bundesländer und damit den Staat selbst handelt.

Anders regelt dies die Satzung der ITEOS, ebenfalls eine Anstalt des öffentlichen Rechts, die baden-württembergische Kommunen bei der IT-Dienstleistung unterstützt. Nach § 2 Abs. 2 der Satzung besteht keine Haftung der Träger für Verbindlichkeiten der ITEOS gegenüber Dritten. Gleichwohl sind die Träger aber verpflichtet, die ITEOS mit den zur Aufgabenerfüllung notwendigen finanziellen Mitteln auszustatten und für die Dauer ihres Bestehens funktionsfähig zu halten.

Auch IT-Dienstleister, die als Landes- bzw. kommunaler Eigenbetrieb ausgestaltet sind, wie die Hessische Zentrale für Datenverarbeitung oder der Landesbetrieb Daten und Information in Rheinland-Pfalz, sind finanziell von Natur aus vollumfänglich abgesichert. Hierbei handelt es sich um rechtlich unselbständige Teile der Landesverwaltung. Privaten IT-Dienstleister fehlt es an einer vergleichbaren institutionellen Garantieebene.

Wenn sich die öffentliche Hand der Rechtsform der GmbH bedient, wie im Falle der Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ M-V) GmbH, bleibt das Niveau der Absicherung ebenfalls regelmäßig hinter dem öffentlich-rechtlicher Rechtsformen zurück. Auch die GmbH in öffentlicher Hand haftet nur in Höhe des Stammkapitals, für die DVZ M-V GmbH etwa 2.000.000 Euro. Eine darüber hinausgehende Verpflichtung der Gesellschafter besteht nicht.

In diesem Zusammenhang muss weiter berücksichtigt werden, dass der Daseinszweck öffentlich-rechtlich verfasster IT-Dienstleister, parallel zu kommunal-

[124] *Kemmler*, Die Anstaltslast, S. 101 ff.; *Müller*, in: H. J. Wolff/Bachof/Stober/Kluth, Verwaltungsrecht II, § 86 Rn. 19.

[125] BVerwG NJW 1987, 3017 (3019).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

wirtschaftlichen Regelungsgrundsätzen,[126] nicht allein in der Gewinnerzielung liegen darf. Für Dataport ist dies in § 11 Abs. 1 S. 2 des Dataport-Staatsvertrags bestimmt. Indem dort festgehalten ist, dass die Erzielung von Gewinn nicht Zweck der Anstalt ist, wird verhindert, dass sich verschiedene Risiken, die aus dem Ziel der Gewinnmaximierung resultieren, nicht in dem oben beschriebenen Maße realisieren können. Für die Haushalts- und Wirtschaftsführung wird grundsätzlich auf öffentlich-rechtliche Haushaltsordnungen verwiesen, was eine Jahresabschlussprüfung durch Aufsichtsbehörden und eine allgemeine Kontrolle der Wirtschaftsführung durch Rechnungshöfe einschließt. Für Dataport finden sich diese Regelungen in den §§ 11 ff. des Dataport-Staatsvertrags. Für die ITEOS wird in § 11 der Satzung auf die sinngemäße Anwendung der Vorschriften des HGB verwiesen; eine Prüfung erfolgt durch die Gemeindeprüfungsanstalt und auch der Rechnungshof hat das Recht zur Prüfung der Haushalts- und Wirtschaftsführung.

Auch in dieser Hinsicht bestehen damit erhebliche Abweichungen zur Geschäftstätigkeit privater IT-Dienstleister, die sich (in legitimer Weise) an einer privatnützigen Betriebsführung orientieren und auf Gewinnerzielung ausgerichtet sind. Eine Prüfung durch den Landesrechnungshof kann auch bei einer GmbH in öffentlicher Hand vorgesehen sein, wie es etwa § 5 DVZG M-V vorsieht. In dem konkreten Beispiel regte der Landesrechnungshof allerdings an, zu prüfen, ob es wirtschaftlicher ist, den Betrieb des Landesrechenzentrums auf einen zentralen Dienstleister innerhalb der Landesverwaltung zu verlagern.[127]

(2) Rechtliche Aufsichts- und Einflussmöglichkeiten

Daneben werden Risiken der Datenübermittlung in private Hoheitsbereiche wie gesehen durch fehlende Aufsichts- und Einflussmöglichkeiten begründet.

IT-Dienstleister, die von der öffentlichen Hand getragen werden, unterliegen einer unmittelbaren Grundrechts- und Gesetzesbindung und handeln im Gemeinwohlinteresse. Diese Anforderungen, die regelmäßig aus gesetzlichen Regelungen folgen, sind im Rahmen einer Vielzahl von Amtspflichten bei der konkreten Aufgabenwahrnehmung zu berücksichtigen. Institutionalisiert werden diese Amtspflichten im Falle einer Anstalt des öffentlichen Rechts durch die Verbindung zum Träger. Im Rahmen dieser Verbindung bestehen erhebliche Einwirkungsmöglichkeiten des Trägers auf die Anstalt. So kann die Einhaltung von Amtspflichten bei öffentlichen Dienstleistern in Form einer Anstalt des öffentlichen Rechts grundsätzlich im Wege der Rechtsaufsicht geltend gemacht werden.

Für Dataport ist dies etwa in § 10 S. 1 des Dataport-Staatsvertrags vorgesehen. Über § 52 LVwG ergibt sich für diesen Zweck die Anwendung der kommunalrechtlichen Rechtsaufsicht nach §§ 122 ff. GO SH. Dies umfasst ein Auskunftsrecht

[126] *Gern/Brüning*, Deutsches Kommunalrecht, Rn. 1001; *Knauff*, in: Schmidt/Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, § 6 Rn. 77.

[127] Landesrechnungshof Mecklenburg-Vorpommern, Jahresbericht 2019, Teil 1, S. 57.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

(§ 122 GO SH), ein Beanstandungsrecht mit der Möglichkeit, bei rechtswidrigem aktivem Tun einstweilige Anordnungen zu erlassen (§ 123 GO SH), ein Anordnungsrecht bei rechtswidrigem Unterlassen mit der Möglichkeit der Ersatzvornahme (§§ 124, 125 GO SH) sowie als ultima ratio sogar das Recht, einen Beauftragten zu bestellen, der anstelle der satzungsmäßig vorgesehenen Organe Aufgaben der Anstalt wahrnimmt (§ 127 GO SH). Auch für den LDI RhPf ist in § 3 des Landesgesetzes über die Errichtung des Landesbetriebs Daten und Information eine Dienst- und Fachaufsicht vorgesehen, die grundsätzlich durch das Ministerium für Inneres und Sport wahrgenommen wird.

Träger staatlicher Gewalt, die sich eines von öffentlicher Hand getragenen IT-Dienstleisters bedienen, können über ihre Aufsichtsbehörden zugleich Aufsichtsmaßnahmen gegenüber dem IT-Dienstleister beeinflussen, weil die jeweiligen Aufsichtsbehörden typischerweise identisch sind. Diese Behördenidentität bietet darüber hinaus tatsächliche soziale, nicht juristisch abbildbare Verbindungen, die die Effektivität der Aufsicht über einen von öffentlicher Hand getragenen IT-Dienstleister in der Praxis erheblich steigern. Außerdem sind Träger staatlicher Gewalt, die einen solchen IT-Dienstleister in Anspruch nehmen, typischerweise über ihre Verbände auch in den Aufsichtsgremien des IT-Dienstleisters vertreten. So bestimmt § 4 der Dataport Satzung, dass (unter anderem) jeweils Vertreter der Bundesländer, die die Anstalt tragen, dem Verwaltungsrat angehören. Auch die ITEOS in Baden-Württemberg verfügt nach § 6 ihrer Satzung über solch einen Verwaltungsrat, dem vor allem Vertreter der tragenden Zweckverbände angehören. In vergleichbarer Weise verfügt LDI RhPf nach § 4 des Errichtungsgesetzes über einen Beirat, wobei die dortigen Mitglieder – da es sich um eine unselbständige Einrichtung des Landes handelt – vor allem aus der Legislative stammen.

Wenn ein IT-Dienstleister der öffentlichen Hand nicht als Anstalt des öffentlichen Rechts, sondern privatrechtlich als GmbH organisiert ist, wie z. B. die DVZ M-V GmbH, bestehen ebenfalls Einwirkungsmöglichkeiten. Diese sind aber nicht öffentlich-rechtlich geprägt und bestehen innerhalb der gesellschaftsrechtlichen Organbeziehungen.

Für die einzelnen Mitarbeiter eines IT-Dienstleisters in öffentlicher Hand können gesetzlich umfangreiche Sicherheitsüberprüfungen vorgesehen sein, wenn diese Zugriff auf sensible Daten erlangen und so mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen. Der Dataport-Staatsvertrag verweist dazu in § 15 Abs. 4 auf das Hamburgische Sicherheitsüberprüfungsgesetz.

Gegenüber juristischen Personen des Privatrechts bestehen im Rahmen einer Auftragsverarbeitung nach Art. 28 Abs. 3 S. 2 lit. h DSGVO Informations- und Inspektionsrechte, doch bleiben diese tätigkeitsbezogenen Möglichkeiten hinter den Einfluss- und Gestaltungsmöglichkeiten einer öffentlich-rechtlichen Aufsicht zurück. Eine andere Ausgestaltung fand sich aber in § 80 Abs. 2 S. 3, 4 SGB X a.F. Die Regelung enthielt nähere Vorgaben für die Auftragsverarbeitung von Sozialdaten. Danach war der Auftraggeber verpflichtet, erforderlichenfalls Weisungen zur Er-

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

gänzung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu erteilen. Flankiert wurde diese Befugnis durch die Verpflichtung des Auftraggebers, sich vor Beginn der Auftragsverarbeitung und anschließend regelmäßig von der Umsetzung der getroffenen Maßnahmen zu überzeugen. Die bereichsspezifische Regelung des § 80 Abs. 2 S. 3, 4 SGB X a.F. fiel aber mit der Implementierung der DSGVO in die nationale Rechtsordnung weg. Die stattdessen eingreifenden Regelungen der DSGVO verpflichten Verantwortliche und Auftragsverarbeiter gleichermaßen. Entscheidend dafür sind verschiedene Sachkriterien. Ein pauschales Weisungsrecht des Verantwortlichen findet sich dort nicht mehr. Dies macht zugleich deutlich, dass die DSGVO als allgemeines Regelwerk spezifische Wege der bisherigen Rechtslage in ihrer Vielfalt kaum übernehmen kann, sondern auf generelle Lösungen setzt.

Im Falle einer Auftragsverarbeitung sind nach der DSGVO zwar unabhängige Aufsichtsbehörden vorgesehen (Art. 51 ff. DSGVO), die auch das Handeln privater IT-Unternehmen überwachen. Hinsichtlich der nichtöffentlichen Stellen konkretisieren die § 40 ff. BDSG die Befugnisse der Aufsichtsbehörden. So sind diesen nach § 40 Abs. 4 BDSG auf Verlangen zur Erfüllung ihrer Aufgaben erforderliche Auskünfte zu erteilen. Nach Abs. 5 sind Personen, die von der Aufsichtsbehörde beauftragt sind, befugt, zur Aufgabenerfüllung Grundstücke und Geschäftsräume des privaten IT-Dienstleisters zu betreten und ihnen ist Zugang zu allen Datenverarbeitungsanlagen und -geräten zu gewähren. Hinzu kommen bei der Auftragsverarbeitung Informationsverpflichtungen des Auftragsverarbeiters nach Art. 28 Abs. 3 S. 2 lit. h DSGVO.

Im Vergleich zu den Aufsichtsmöglichkeiten gegenüber öffentlichen IT-Dienstleistern lassen sich im Rahmen des Datenschutzrechts aber zwei wesentliche Unterschiede ausmachen. Zum einen sind die Mittel, die einer Aufsichtsbehörde gegenüber privaten IT-Dienstleistern zur Verfügung stehen, erheblich eingeschränkt. Nach Art. 83 DSGVO, § 41 Abs. 1 BDSG können bei Verstößen gegen näher bestimmte Regelungen der DSGVO, zu denen auch die Vorschriften über die Auftragsverarbeitung zählen, Geldbußen verhängt werden. Weitergehende Befugnisse, unmittelbar auf das Handeln privater IT-Dienstleister einzuwirken, bestehen aber nicht. Die bestehenden Möglichkeiten der Aufsichtsbehörden knüpfen außerdem an den Anwendungsbereich der DSGVO an und damit gemäß Art. 2 Abs. 1 DSGVO an die Verarbeitung personenbezogener Daten. Praktisch wird es dabei häufig zu Überschneidungen mit Gefahren für die Funktionsfähigkeit der Verwaltung kommen; nicht jedes dieser Risiken geht aber zwangsläufig mit der Verarbeitung personenbezogener Daten und einem Rechtsverstoß nach der DSGVO einher. Vielmehr können Gefahren bestehen, bei denen zweifelhaft ist, ob die Aufsichtsbehörden im Rahmen der DSGVO überhaupt zuständig sind. In diesen Konstellationen kann die privatautonome Dispositionsbefugnis und die Möglichkeit, Eigeninteressen zu verfolgen, für Unternehmen in privater Hand besondere Bedeutung bekommen.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Personen, die bei privaten IT-Dienstleistern beschäftigt sind und die im Rahmen einer Auftragsverarbeitung zur Verarbeitung personenbezogener Daten befugt sind, müssen sich nach Art. 28 Abs. 3 lit. b DSGVO zumindest zur Vertraulichkeit verpflichtet haben.[128] Nach lit. h müssen IT-Dienstleister außerdem alle erforderlichen Informationen zum Nachweis der Einhaltung der ihnen obliegenden Pflichten zur Verfügung stellen und Überprüfungen einschließlich Inspektionen ermöglichen. Auf die praktischen Hürden, die sich dabei stellen können, wurde schon hingewiesen.[129] Besonders hervorzuheben ist hierbei der Einwand grundrechtlich geschützter Geschäfts- und Betriebsgeheimnisse. Das Handeln privater IT-Dienstleister ist typischerweise dadurch gekennzeichnet, dass es Kunden bzw. Dritten schon an Kenntnissen über betriebsinterne Prozesse fehlt und diese auch nur schwerlich zu erlangen sind. Mitunter lässt sich bei großen IT-Dienstleistern für Externe auch nicht erkennen, in welchem nationalen Hoheitsbereich Daten sich befinden. Im Gegensatz dazu haben öffentliche IT-Dienstleister nicht nur die Verpflichtungen aus der DSGVO zu erfüllen, sie unterstehen zusätzlich auch einer behördlichen Rechtsaufsicht, die besondere Befugnisse für sich in Anspruch nehmen kann.

bb) Ausschluss Privater als Konsequenz der Verwaltung als kritischer Infrastruktur

Daten haben für die Verwaltung einen elementaren Wert. Der Staat muss deshalb gewährleisten, dass Daten, die die Verwaltung für die Wahrnehmung ihrer Aufgaben benötigt, jederzeit und in inhaltlich einwandfreier Weise zur Verfügung stehen. Aufgrund der Bedeutung, die digitale Informationstechnologien mittlerweile für alltägliche Arbeitsprozesse haben, gerade auch in der Verwaltung, ist der reibungslose Zugriff auf die notwendigen Daten zu einer unabdingbaren Grundvoraussetzung für die Realisierung der Staatsfunktion Verwaltung geworden.[130] Auch die ordnungsgemäße Dokumentation des Verwaltungshandelns und die spätere Möglichkeit, hierauf zuzugreifen, sind zwingende Voraussetzungen für die Funktionsfähigkeit der Verwaltung. Dadurch werden Wissensquellen für zukünftiges Verwaltungshandeln erschlossen, die eine einheitliche und stringente und damit rechtsstaatliche Verwaltungsführung sicherstellen und die Ausübung der Staatsgewalt unabhängig vom Wissen Einzelner ermöglichen.[131] Diese Verpflichtungen lassen sich auch – nicht zuletzt aufgrund ihrer Auswirkungen auf die Möglichkeiten bürgerlichen Rechtsschutzes – bei Fehlen einer einfachgesetzlichen Regelung unmittelbar dem Rechtsstaatsprinzip entnehmen.[132] Solche Anforderungen an die Verwaltung gelten ungeachtet der Frage, ob man die staatliche Datenverwendung im

[128] Vgl. oben C. III. 2. b) dd).

[129] Vgl. oben C. III. 2. b) bb).

[130] Vgl. *Gitter/Meißner/Spauschus*, DuD 2016, 7 (7).

[131] BVerfG NJW 1983, 2315 (2315); *Grundmann/Greve*, NVwZ 2015, 1726 (1726).

[132] BVerfG NJW 1983, 2315 (2315); *Kallerhoff/Mayen*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, § 29 Rn. 30; *Grundmann/Greve*, NVwZ 2015, 1726 (1726).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Einzelfall als eine bloße Unterstützungsfunktion oder eigenständige Aufgabe einordnet. Praktisch verliert die Verwaltung die Fähigkeit zur Aufgabenwahrnehmung auf breiter Linie, sobald die Nutzung damit im Zusammenhang stehender Daten nicht mehr gesichert ist.

In den letzten Jahren haben der europäische und nationale Regelungsgeber die Bedeutung bestimmter Einrichtungen, Anlagen, Tätigkeiten oder Dienstleistungen für das Gemeinwesen anerkannt und Vorschriften zum Schutz und zur Abhärtung der in diesem Zusammenhang verwendeten Informationstechnologien erlassen. Dies lag auch daran, dass Störungen und Sicherheitsvorfälle erheblich zugenommen haben.[133] Im nationalen Recht haben sich die Anforderungen an solche sog. kritischen Infrastrukturen durch das IT-Sicherheitsgesetz[134] vor allem im BSI-Gesetz niedergeschlagen. Nach § 2 Abs. 10 BSI-Gesetz, konkretisiert durch die Bestimmungen der BSI-KritisV, sind kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit eintreten würden.

Staatlich betriebene Einrichtungen, Anlagen oder Teile davon, die nicht in einem der benannten Sektoren tätig sind, sondern genuine Aufgaben staatlicher Verwaltung wahrnehmen (und dasselbe gilt für Rechtsprechung und Gesetzgebung), werden von den gesetzlichen Regelungen nicht erfasst, sondern sind Gegenstand originärer Regelungsbefugnisse staatlicher Stellen, auf Bundesebene etwa des Bundesamts für Sicherheit in der Informationstechnik. Die fehlende begriffliche Einordnung als kritische Infrastruktur darf aber nicht darüber hinwegtäuschen, dass auch durch einen Ausfall von Verwaltungsfunktionen erhebliche Gefährdungen der öffentlichen Sicherheit eintreten können – bis hin zu einem vollständigen Ausfall staatlicher Funktionen. Aus dem Prinzip der Gewährleistungsverantwortung ergeben sich eigenständige Konsequenzen, die an die Stelle der Anforderungen treten, die gesetzlich an kritische Infrastrukturen gestellt werden.

Insofern bestehen zwangsläufig Überschneidungen zu der Begründungssäule der obligatorischen Staatsaufgaben, wobei der Aspekt der Gewährleistungsverantwortung nach innen auch Konstellationen erfassen kann, in denen keine obligatorischen Staatsaufgaben in Rede stehen.

Als Folge der grundlegenden Bedeutung von Daten für die Wahrnehmung staatlicher Verwaltungsaufgaben sowie den praktischen Auswirkungen ihrer Wesensmerkmale kann es aufgrund der staatlichen Gewährleistungsverantwortung

[133] Erwägungsgrund Nr. 1 f. Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, NIS-Richtlinie (EU) 2016/1148.

[134] Allgemein hierzu *Gitter/Meißner/Spauschus*, DuD 2016, 7; *Pohlmann*, DuD 2016, 38; *Könen*, DuD 2016, 12; *Grudzien*, DuD 2016, 29.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

unter bestimmten Umständen notwendig sein, einen (unmittelbaren oder mittelbaren) Zugriff auf Daten durch Private zu verhindern und Daten ausschließlich in einem öffentlich-rechtlich geprägten Herrschaftsbereich zu belassen. Würden hingegen in solchen Konstellationen Privaten die Daten übermittelt werden, wäre den Privaten zugleich ein Zugriff auf die Funktionsfähigkeit der staatlichen Verwaltung selbst eingeräumt. Für Private würde sich damit im äußersten Fall faktisch die Möglichkeit ergeben, die Funktionsfähigkeit der staatlichen Verwaltung von ihrem Belieben abhängig zu machen. Es entstünde die Gefahr, dass sich politische Überlegungen, vor allem durch ausländische oder ausländisch beherrschte Unternehmen,[135] oder betriebliche Ziele, etwa im Zusammenhang mit Vertragsverhandlungen, zu einem maßgeblichen Handlungsmotiv aufschwingen. Bestehende rechtliche Vereinbarungen können für die tatsächliche Ausnutzung einer solchen eingeräumten Position keine effektive Sicherung bieten.

Von dieser Facette des Grundsatzes der digitalen Souveränität sind solche Daten erfasst, die für die Funktionsfähigkeit der staatlichen Verwaltung (oder Rechtsprechung bzw. Gesetzgebung) von hoher Bedeutung sind, weil eine Beeinträchtigung ihrer vorgesehenen Nutzung zu erheblichen Defiziten bei der Aufgabenwahrnehmung oder anderen Gefährdungen der öffentlichen Sicherheit führen würde. Eine bloße Unbequemlichkeit im internen Verwaltungsablauf reicht hierfür nicht aus. Vielmehr muss der gewöhnliche Geschäftsgang in besonderem Maße durch die Funktionsbeeinträchtigung gestört werden. Ihre Folgen müssen zu erheblichen Missständen gerade auch in den Außenbeziehungen der Verwaltung führen. Die Erfüllung von Verwaltungsaufgaben dem Bürger gegenüber muss erheblich gestört werden. Dies kann etwa darauf zurückzuführen sein, dass verlorene Daten nicht oder nur unter erheblichen Anstrengungen wiedererlangt werden können oder Daten veröffentlicht werden, so dass die alleinige öffentlich-rechtliche Inhaberschaft aufgehoben wird und deshalb nachteilige Konsequenzen eintreten.

cc) Beispiel: E-Akte in der Verwaltung, § 6 EGovG

Neben den Gerichten öffnet sich auch die Verwaltung mehr und mehr digitalen Informationstechnologien. Begleitet wird dieser Prozess unter anderem durch das E-Government-Gesetz des Bundes (EGovG), das hier exemplarisch betrachtet werden soll. Nach § 6 S. 1 EGovG sollen die Behörden des Bundes ihre Akten elektronisch führen, wobei diese Regelung erst mit Wirkung vom 1. Januar 2020 in Kraft tritt. Für den Fall, dass eine Akte elektronisch geführt wird, ist gemäß § 6 S. 3 EGovG durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden.

[135] Vgl. die Handreichung vom 19. 8. 2014 zum sog. No-Spy Erlass des BMI, O4 – 11032/23#14, S. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Die Grundsätze ordnungsgemäßer Aktenführung müssen uneingeschränkt auch bei elektronischen Akten eingehalten werden.[136] Für die E-Akte bedeutet dies, dass neben der Verpflichtung, Akten zu führen (Gebot der Aktenmäßigkeit), diese vollständig, nachvollziehbar, inhaltlich wahrheitsgetreu und langfristig verfügbar sein müssen.[137] Aus den Akten darf nichts entfernt werden und sie dürfen nicht verfälscht werden, so dass die Authentizität und Integrität gesichert ist.[138] Außerdem muss die Vertraulichkeit und Löschbarkeit gewährleistet werden.[139] Diese Anforderungen, die sich aus § 6 S. 3 EGovG ergeben, sind Ausdruck einer Gewährleistungsverantwortung nach innen, weil sie zum Ziel haben, die Funktionsfähigkeit der Verwaltung sicherzustellen. Abhängig von dem konkreten Dateninhalt kann sich deshalb die Unzulässigkeit einer Datenübertragung in private Herrschaftssphären ergeben.

Selbstverständlich gelten diese Grundsätze der ordnungsgemäßen Aktenführung auch für die schon angesprochenen elektronischen Prozessakten bei Gericht. Das obige Beispiel der elektronischen Prozessakten sollte jedoch die Ermittlung und Konsequenzen eines integralen Bestandteils obligatorischer Staatsaufgaben darstellen. Für die E-Akte in der Verwaltung lässt sich nicht pauschal ihre Bedeutung als integraler Bestandteil einer obligatorischen Staatsaufgabe annehmen. Ihr Beispiel veranschaulicht aber, dass es über obligatorische Staatsaufgaben hinaus weitere Begründungsansätze gibt, um den Grundsatz der digitalen Souveränität abzuleiten.

b) Gewährleistungsverantwortung nach außen

Neben diese nach innen, primär auf die Funktionsfähigkeit der Verwaltung selbst gerichtete Gewährleistungsverantwortung tritt eine Gewährleistungsverantwortung nach außen.

aa) Datensicherheit bei personenbezogenen Daten

Die Datensicherheit bei personenbezogenen Daten betrifft das Staat-Bürger-Verhältnis und zielt insbesondere auf die Gewährleistung von Grundrechten ab, vor allem im Hinblick auf den Schutz personenbezogener Daten (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG).

(1) Konkrete Betrachtung der Einzelfallumstände

Die Konkretisierung der Gewährleistungsverantwortung in dieser Konstellation muss zwangsläufig an die Umstände des Einzelfalls anknüpfen, also insbesondere

[136] *Grundmann/Greve*, NVwZ 2015, 1726 (1727).

[137] BT-Drs 17/11473, S. 38.

[138] BT-Drs 17/11473, S. 38.

[139] BT-Drs 17/11473, S. 38.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

den konkreten Dateninhalt sowie dessen Bedeutung für den Einzelnen. Das Ableiten allgemeiner Maßstäbe wird dadurch erschwert.

Im Verhältnis zum Bürger folgen die schwerwiegendsten Risiken aus einer Offenbarung personenbezogener Daten gegenüber Dritten. Diesen Risiken kann zwar durch eine Datenverschlüsselung entgegengewirkt werden. Kommt es aber zu einer Offenbarung, wird man dies regelmäßig als eigenständige Rechtsbeeinträchtigung der Betroffenen bewerten müssen.[140] Bei einer zumindest mittelbaren Zugriffsmöglichkeit Privater auf personenbezogene Daten (etwa durch das Verfügen über den physischen Datenträger) kann es weiter zu einer Nichtverfügbarkeit oder Korruption personenbezogener Daten kommen, die erhebliche Beeinträchtigungen bürgerlicher Rechtspositionen nach sich ziehen kann.

Ein Schutz der grundrechtlichen Positionen muss insbesondere deshalb gewährleistet werden, weil sich der Bürger der rechtsverbindlich angeordneten Datenerhebung und -verarbeitung durch den Staat regelmäßig erheblich schwerer entziehen kann, als wenn dies durch andere Private erfolgt.

(2) Auftragsverarbeitung und angemessenes Schutzniveau

Konstellationen, in denen Privaten Zugriff auf staatliche Daten ermöglicht wird, können grundsätzlich als Formen der Auftragsverarbeitung eingeordnet werden. Nichts anderes ist für öffentliche IT-Dienstleister anzunehmen. Die Regeln der DSGVO sind in höchstem Maße vereinheitlicht. Die Regelung des Art. 28 DSGVO zur Auftragsverarbeitung gilt für private wie öffentliche IT-Dienstleister gleichermaßen. Sie kommt zur Anwendung bei einer Auftragsverarbeitung zwischen Privaten, zwischen öffentlich-rechtlichen Stellen, aber auch wenn eine öffentlich-rechtliche Stelle Daten von einem Privaten verarbeiten lässt und umgekehrt. Auch hinsichtlich der Art der Daten finden die Regelungen gleichermaßen pauschal Anwendung; Sonderregelungen für besondere Kategorien personenbezogener Daten fehlen grundsätzlich im Recht der Auftragsverarbeitung. Zweifelhaft ist deshalb, ob diese pauschalen und allgemeingültigen Vorschriften hinreichend bestimmt die Anforderungen erfassen, die sich gerade für eine Datenweitergabe von öffentlich-rechtlichen Stellen an Private ergeben.

Die Auftragsverarbeitung nach § 11 BDSG a.F. sah eine Vereinbarung zwischen Auftraggeber und Auftragnehmer vor, in der verschiedene Aspekte, die sich unter anderem gegen die beschriebenen Risiken beim Outsourcing richten, festzulegen waren. Auch die Auftragsverarbeitung nach Art. 28 DSGVO enthält solche Regelungen, weist jedoch ein erheblich höheres Regelungsniveau auf, als das bisherige BDSG. So muss nach Art. 28 Abs. 1 DSGVO der Auftragsverarbeiter hinreichend Garantien bieten, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt. Diese werden unter anderem in Art. 28 Abs. 3 DSGVO näher

[140] Vgl. BVerfGE 100, 313 (366 f.); 125, 206 (310).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

konkretisiert. Dazu gehören etwa Dokumentationspflichten (lit. a), Regelungen zur Vertraulichkeit einbezogener natürlicher Personen (lit. b), Löschpflichten (lit. g) oder Inspektions- und Prüfpflichten (lit. h). Art. 32 DSGVO enthält nähere Vorgaben für die Datensicherheit im Falle einer Auftragsverarbeitung, unter anderem hinsichtlich der Datenverfügbarkeit.

Zur Annäherung an das Niveau der Datensicherheit, das für personenbezogene Daten in staatlicher Hand zu erfüllen ist, kann die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung herangezogen werden.[141] Die Indienstnahme Privater zur Speicherung solcher Daten, die von den Privaten zuvor selbst erhoben worden waren, zum Zwecke einer möglichen späteren Auswertung durch den Staat, war auch deshalb verfassungswidrig, weil die Anforderungen zur Datensicherheit bei den Privaten nicht ausreichend waren. Die von den Privaten vorzunehmenden Schutzmaßnahmen dürfen nicht einer „freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten" unterworfen werden, vielmehr sind gesetzliche Regelungen erforderlich, die einen „besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben".[142]

Die Regelungen zur Datensicherheit nach Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO enthalten abstrakte Kriterien, die bei der Festlegung konkreter Maßnahmen zur Datensicherheit im Einzelfall zu berücksichtigen sind, so der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten natürlicher Personen. Die Kosten, die von Auftragsverarbeitern für die Gewährleistung der Sicherheit ihnen anvertrauter Daten in zumutbarer Weise aufzuwenden sind, hängen nach der Konzeption des Art. 32 Abs. 1 DSGVO von den Umständen des Einzelfalls ab, zum einen von der Eintrittswahrscheinlichkeit und zum anderen von der Schadenshöhe.[143] Dabei ergibt sich für die Schadenshöhe, dass das Sicherheitsniveau umso höher sein muss, je sensibler die betroffenen personenbezogenen Daten sind.[144]

Um eine „freie" Abwägung mit wirtschaftlichen Gesichtspunkten, wie es das Bundesverfassungsgericht in der Entscheidung zur Vorratsdatenspeicherung bemängelt hatte, handelt es sich hierbei nicht. Anders aber als in der gesetzlichen Regelung des § 113a TKG a.F., die der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung zugrunde lag, werden mit den Implementierungskosten wirtschaftliche Aspekte in Art. 32 DSGVO ausdrücklich als Abwägungsposition benannt. Das Kriterium der Implementierungskosten dient dazu, die wirtschaftlichen

[141] BVerfGE 125, 260.

[142] BVerfGE 125, 260 (326 f.).

[143] Vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 50.

[144] *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 51.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Belange der datenverarbeitenden Stellen zu berücksichtigen.[145] Die datenverarbeitenden Stellen sind dabei nicht in unbegrenztem Maße, sondern nur auf das wirtschaftlich Zumutbare verpflichtet; die Grenze der Unzumutbarkeit ist dabei nicht erst bei einem finanziellen Aufwand erreicht, der existenzgefährdend ist.[146] Der finanzielle Aufwand, der mit den Sicherheitsmaßnahmen einhergeht, muss verhältnismäßig sein.[147] Erscheint eine denkbare Sicherungsmaßnahme angesichts der möglichen Schadenshöhe unverhältnismäßig, muss dies nicht dazu führen, dass eine Datenverarbeitung nicht möglich ist, sondern kann auch dazu führen, dass das Schutzniveau angepasst wird.[148]

Fraglich ist, ob in dieser Situation die Abwägungsbelange von privaten und öffentlichen IT-Dienstleistern, die im öffentlichen Auftrag agieren, identisch sind oder strukturelle Unterschiede zum Ausdruck bringen. Dies könnte nahe liegen, da öffentliche IT-Dienstleister regelmäßig dem Gemeinwohl verpflichtet sind, private IT-Dienstleister hingegen grundsätzlich nach Gewinn und erfolgreichem wirtschaftlichen Handeln streben. Bei Privaten sind diese Handlungsmotive durch die Berufsfreiheit grundrechtlich geschützt. Man könnte deshalb meinen, dass es nicht ausgeschlossen ist, diese Aspekte als rechtlich relevante Kriterien in die Abwägung einzuführen, während sich öffentliche IT-Dienstleister auf eine vergleichbare grundrechtlich abgesicherte Abwägungsposition hingegen nicht berufen können. Die Konsequenz wäre, dass für Private im Vergleich zu öffentlichen Stellen bei der notwendigen Ermittlung des erforderlichen und zumutbaren Aufwands in einem erhöhten Maße die Implementierungskosten und damit die Auswirkungen auf den wirtschaftlichen Erfolg zu berücksichtigen wären.

Dies würde aber voraussetzen, das notwendige Schutzniveau individuell abhängig vom Verantwortlichen bzw. der verarbeitenden Stelle zu bestimmen. Die Folge könnte sein, dass auch innerhalb eines Auftragsverhältnisses das Schutzniveau

[145] Verbreitet wird in diesem Zusammenhang lediglich auf die ökonomischen Interessen des Verantwortlichen hingewiesen, ohne die des Auftragsverarbeiters gesondert zu benennen, *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 32 Rn. 11; *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 84. Zwar richten sich die Anforderungen zur Datensicherheit in erster Linie an den Verantwortlichen, doch wird dadurch auch ein möglicher Auftragsverarbeiter verpflichtet. Art. 32 DSGVO richtet sich in selbständiger Art und Weise sowohl an Verantwortlichen als auch einen etwaigen Auftragsverarbeiter, *Piltz*, in: Gola (Hrsg.), DSGVO, Art. 32 Rn. 7; *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 32 Rn. 1, 4. Bei einer marktorientierten Betrachtung ist zu berücksichtigen, dass der Auftragsverarbeiter seine Dienstleistung zu einem bestimmten Marktpreis anbietet und hierfür sind die ihm entstehenden Kosten ein maßgeblicher Faktor.

[146] OLG Hamburg NJW 2006, 310 (313); *Hladjk*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 32 Rn. 5; *Piltz*, in: Gola (Hrsg.), DSGVO, Art. 32 Rn. 20; *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 60.

[147] *Piltz*, in: Gola (Hrsg.), DSGVO, Art. 32 Rn. 13, 20; *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 84.

[148] *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 84 f.; *Kramer/Meints*, in: Auernhammer, DSGVO/BDSG, Art. 32 DSGVO Rn. 34.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

unterschiedlich ausgeprägt wäre. Das würde jedoch der individuellen wirtschaftlichen Leistungsfähigkeit einen zu großen Stellenwert einräumen, könnte eine schlechte Betriebsführung durch abgesenkte Anforderungen belohnen und würde zu Unsicherheiten bei den Beteiligten über das notwendige Schutzniveau führen. Anstelle einer Berücksichtigung der individuellen wirtschaftlichen und finanziellen Verhältnisse ist das gebotene Schutzniveau deshalb mittels einer objektiven Betrachtung bestimmen.[149]

Für die Frage der Datenübertragung an private IT-Dienstleister muss daneben aber auch die Bedeutung der Daten berücksichtigt werden. Eine zulässige Auftragsverarbeitung kann auch hochsensible Daten erfassen, wie etwa besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO).[150] Eine ausdrückliche absolute Grenze für die Einbeziehung Privater (bzw. Auftragsverarbeiter) durch den Staat, die sich beispielsweise anhand der Bedeutung der Daten für den einzelnen Betroffenen ergeben könnte, fehlt den gesetzlichen Regelungen. Dies stellt jedoch nicht davon frei, abzuwägen, ob es angemessen ist, Private einzubeziehen.

Diese Frage zu bejahen setzt voraus, dass es für den Staat in der konkreten Situation möglich ist, ein angemessenes Schutzniveau zu gewährleisten. Im Rahmen einer Gewährleistungsverantwortung ergibt sich dies maßgeblich aus grundrechtlichen Schutzpflichten. Nach dem Untermaßverbot muss der Gesetzgeber solche Vorkehrungen treffen, die für einen angemessenen und wirksamen Schutz ausreichend sind und auf sorgfältigen Tatsachenermittlungen und vertretbaren Einschätzungen beruhen.[151]

Wenn Träger staatlicher Gewalt Daten, die Grundrechtsträger betreffen und von hochsensibler Natur sind, in den Einflussbereich privater IT-Dienstleister geben, muss das Recht auf informationelle Selbstbestimmung hinreichend geschützt sein. Eine Gefahr für diese grundrechtliche Position mag typischerweise durch eine unbefugte Einsichtnahme und Veröffentlichung bestehen. Insofern darf man nicht außer Acht lassen, dass das Sicherheitsniveau im Einzelfall in der Praxis bei privaten IT-Dienstleistern auch höher sein kann als bei öffentlichen IT-Dienstleistern. Im IT-Bereich existieren Unternehmen, die eine erhebliche Marktmacht erlangt haben und

[149] *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 25 DSGVO Rn. 42; *Kramer/Meints*, in: Auernhammer, DSGVO/BDSG, Art. 32 DSGVO Rn. 35.

[150] Vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 32 DSGVO Rn. 51.

[151] BVerfGE 88, 203 (254); 109, 190 (247); *Dreier*, in: ders. (Hrsg.), GG, Vorb. Rn. 103; *Jarass*, in: Merten/Papier (Hrsg.), HGR II, § 38 Rn. 32; *Jarass/Pieroth*, GG, Vorb. vor Art. 1 Rn. 56. Das Bundesverfassungsgericht geht davon aus, dass eine Schutzpflicht verletzt ist, „wenn die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder erheblich dahinter zurückbleiben", BVerfGE 92, 26 (46); 109, 190 (247); leicht abgewandelt ebenso BVerfGE 77, 170 (215); vgl. auch BVerfGE 88, 203 (251 ff.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

häufig hängt damit auch ein Zuwachs an Ressourcen zusammen, der sich auf das Niveau der Datensicherheit positiv auswirken kann.

Auch wenn in dieser Hinsicht bei privaten IT-Dienstleistern ein geringes Risiko bestehen sollte, wird dieses durch die erhebliche Schadenshöhe, wenn höchstpersönliche und sensible Daten betroffen sind, überlagert. Das Eröffnen privater Einwirkungsmöglichkeiten, die nicht durch Grundrechtsbindung und Gesetzmäßigkeit der Verwaltung geprägt sind, führt zu einer Diffusion von Verantwortlichkeiten durch die unterschiedlichen berührten Regelungssphären. Die Folge ist, dass sich auf vielfältige Art und Weise die Modalitäten und Kontrollmöglichkeiten für den Umgang mit Daten lockern.[152] Die generell bestehenden Risiken, die sich mit jeder Weitergabe von Daten ergeben,[153] nehmen unter diesen Bedingungen noch zu. Schon im Allgemeinen können bloße Grundrechtsgefährdungen nach der Rechtsprechung des Bundesverfassungsgerichts eine staatliche Rechtfertigungslast begründen, wenn sich eine Realisierung der Gefahr unter Berücksichtigung der Bedeutung des bedrohten Schutzguts und dem drohenden Schaden hinreichend konkret abzeichnet.[154] Dies gilt im Besonderen für das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Da dieses Grundrecht schon an den Schritten der Datenerhebung-, speicherung und -verarbeitung ansetzt, die regelmäßig lediglich Grundlage für eine konkrete Beeinträchtigung durch die spätere Verwendung sind, wendet sich das Grundrecht bereits strukturell unmittelbar gegen Grundrechtsgefährdungen.[155] Durch das Grundrecht auf informationelle Selbstbestimmung sollen daneben insbesondere auch Einschüchterungen verhindert werden, die entstehen, wenn für den Einzelnen nicht mehr erkennbar ist, wer über Daten, welche die eigene Person betreffen, verfügen kann und welche Folgen daraus resultieren können.[156]

Selbst im Falle einer öffentlich-rechtlichen Tätigkeit in der Rechtsform der GmbH sind diese Gefahren nicht vollständig gebannt. So hat der Landesrechnungshof Mecklenburg-Vorpommern für die DVZ M-V GmbH festgestellt, dass für diese nicht zwangsläufig dieselben Sicherheitsvorgaben wie für bestimmte Bereiche der Landesverwaltung gelten.[157] Im konkreten Fall bedurfte es vielmehr entweder einer gesonderten gesetzlichen Regelung oder einer besonderen vertraglichen Regelung.

Grundsätzlich kommt die Rechtfertigung einer solchen Grundrechtsgefährdung nicht in Betracht. Zwar ist eine Kostenersparnis ein häufiges Motiv für die Beauftragung privater IT-Dienstleister. Doch werden die Kosten für eine entsprechende

---

[152] Vgl. oben C. III. 2. b).

[153] Vgl. oben C. III. 2. a) bb).

[154] BVerfGE 49, 89 (141 f.); 51, 324 (346 f.); 66, 39 (58); 77, 170 (220); *Sachs*, in: ders. (Hrsg.), GG, Vor Art. 1 Rn. 95; *Ruschemeier*, Der additive Grundrechtseingriff, S. 115 f.

[155] BVerfGE 115, 320 (341 f.); 120, 378 (397); BVerfG NVwZ 2016, 53 Rn. 11; *Poscher*, in: Gander/Perron/Poscher u. a. (Hrsg.), Resilienz in der offenen Gesellschaft, S. 167 (181 ff.).

[156] Vgl. BVerfGE 65, 1 (42); 113, 29 (46); 115, 166 (188); 115, 320 (341 f.).

[157] Landesrechnungshof Mecklenburg-Vorpommern, Jahresbericht 2019, Teil 1, S. 55 f.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

öffentlich-rechtlich geprägte IT-Dienstleistung regelmäßig nicht derart höher sein, dass damit ein unvertretbarer finanzieller Aufwand verbunden wäre.[158] Mögliche Effektivitätsgewinne durch weiterentwickelte Systeme privater IT-Dienstleister müssten im spezifischen Anwendungsfall dargelegt werden und gegenüber der Grundrechtsgefährdung überwiegen. Denkbar könnte dies ausnahmsweise in solchen Situationen sein, in denen die spezifische Art der Datenverarbeitung durch den Staat selbst nicht vorgenommen werden kann, dies aber gleichzeitig einen wichtigen Zweck verfolgt, wie etwa besondere DNA-Analysen, wobei dies im Einzelfall nach wie vor eine Abwägung mit der Intensität und Konkretheit der Grundrechtsgefährdung voraussetzen würde.

bb) Ausschluss Privater als Konsequenz des Grundrechtsschutzes

Träger staatlicher Gewalt können aufgrund ihrer besonderen Befugnisse in einem bedeutend umfangreicheren Maße auf personenbezogene Daten zugreifen als Private. Dies bewirkt eine erhebliche Grundrechtssensibilität ihres Handelns. Träger staatlicher Gewalt sind deshalb verpflichtet, besondere Sicherheitsanforderungen im Umgang mit personenbezogenen Daten zu erfüllen.

Für den Umgang mit bestimmten Daten in bestimmten Situationen kann sich der ausreichende grundrechtliche Schutz der Betroffenen nur gewährleisten lassen, wenn diese Daten ausschließlich in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben. Maßgeblich für diese Entscheidung kann die Bedeutung der Daten für die Grundrechtswahrnehmung sein, ihr Bezug zu intimen Sachverhalten, ihre persönlichkeitsbezogene Sensibilität oder auch ihre Attraktivität für Dritte. Ein mögliches Kriterium kann auch sein, ob der Staat die Daten im Rahmen von Eingriffsbefugnissen oder auf freiwilliger Basis erhoben hat, wobei im letzteren Fall auch zu berücksichtigen wäre, inwiefern die Datenerhebung für den selbstbestimmten Lebensalltag der Bürger von Bedeutung ist.

Für IT-Dienstleister in privater wie öffentlicher Hand ergeben sich Sicherheitsanforderungen aus den Regeln zur Auftragsverarbeitung, die für beide Kategorien von Akteuren gleichermaßen Anwendung finden. Im Falle einer Übertragung von Daten durch Träger staatlicher Gewalt an Private können diese gesetzlichen Regelungen als Ausdruck einer staatlichen Gewährleistungsverantwortung angesehen werden. Für IT-Dienstleister in staatlicher Hand ergeben sich jedoch weitere Sicherheitsanforderungen aus ihrer unmittelbaren Grundrechts- und Gesetzesbindung.[159] Unter Beachtung dieser zusätzlichen Voraussetzungen erscheint es zweifelhaft, ob die Regeln zur Auftragsverarbeitung in ihrer Pauschalität den Besonderheiten und vielfältigen Ausgestaltungen des Verhältnisses von Trägern staatlicher Gewalt und Privaten stets gerecht werden können. Schon bislang wurden für einzelne Bereiche ungeschriebene Verschärfungen des Rechtsrahmens der Auftragsverar-

[158] Vgl. BVerfGE 77, 84 (110 f.); 81, 70 (91 f.).

[159] Vgl. *Ulmer*, CR 2003, 701 (702).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

beitung angenommen. So wird z. B. eine Vorrangwirkung des Steuergeheimnisses nach § 30 AO anerkannt mit der Folge, dass die Regelungen der Auftragsverarbeitung schon per se keine Anwendung auf diese Konstellation finden.[160] Die Anerkennung solcher Sondersituationen, die die Regeln über die Auftragsverarbeitung suspendieren, ist Ausdruck der staatlichen Gewährleistungsverantwortung.

Es sind also Konstellationen möglich, in denen höchstpersönliche Daten im alleinigen Hoheitsbereich des Staates verbleiben müssen, weil anderenfalls kein angemessener und wirksamer Grundrechtschutz möglich wäre. Bei Trägern staatlicher Gewalt sind personenbezogene Daten vorhanden, die zwar verhältnismäßig beim Bürger erhoben und staatlich verarbeitet werden dürfen, für die aber zugleich nicht in angemessener Art und Weise Privaten irgendwie geartete Zugriffsmöglichkeiten darauf eröffnet werden dürfen.

cc) Beispiele: Datenverarbeitung durch Strafverfolgungsorgane, § 497 StPO, Verarbeitung von Sozialdaten, § 80 Abs. 3 SGB X und Beihilfeakte, § 108 BBG

Ebenso wie Zivilgerichte und die allgemeine Verwaltung nutzen auch Strafverfolgungsorgane mittlerweile flächendeckend elektronische Datenverarbeitung und sind in der Lage, elektronische Akten zu führen. Die am Beispiel elektronischer Prozessakten der Zivilgerichte und E-Akten der Verwaltung dargestellten Erwägungen zur Bedeutung obligatorischer Staatsaufgaben und deren integraler Bestandteile sowie zur Gewährleistungsverantwortung nach innen lassen sich mit Modifikationen auch für die Datenverarbeitung durch Strafverfolgungsorgane heranziehen. Das Beispiel der elektronischen Akten der Strafverfolgungsorgane, vor allem der Staatsanwaltschaft, kann zusätzlich den Aspekt der Gewährleistungsverantwortung nach außen veranschaulichen. Strafakten enthalten regelmäßig eine Fülle höchstpersönlicher Informationen, nicht nur des Verdächtigen bzw. Täters, sondern insbesondere auch von Opfern und Zeugen.[161]

Nach § 497 Abs. 1 StPO, in Kraft getreten zum 1. Januar 2018, dürfen nichtöffentliche Stellen mit der dauerhaften rechtsverbindlichen Speicherung elektronischer Akten nur dann beauftragt werden, wenn eine öffentliche Stelle den Zutritt und den Zugang zu den Datenverarbeitungsanlagen, in denen die elektronischen Akten rechtsverbindlich gespeichert werden, tatsächlich und ausschließlich kontrolliert. Die Gesetzesbegründung geht davon aus, dass ein vollständiger Ausschluss der Beauftragung Privater einen effizienten und wirtschaftlichen IT-Betrieb im Zusammenhang mit der elektronischen Strafakte wesentlich erschweren würde.[162]

---

[160] Vgl. *Alber*, in: in: Hübschmann/Hepp/Spitaler (Hrsg.), AO/FGO, § 30 AO Rn. 16; *Rüsken*, in: Klein, AO, § 30 Rn. 13.

[161] *Ritscher*, in: Satzger/Schluckebier/Widmaier (Hrsg.), StPO, § 497 Rn. 1; *v. Häfen*, in: Graf (Hrsg.), BeckOK StPO, § 496 Rn. 9 f.

[162] BT-Drs. 18/9416, S. 68.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Dafür gibt es tatsächlich aber keine Anzeichen. Die öffentliche Hand betreibt aufgrund einfachgesetzlicher Regelungen effektiv verschiedene IT-Dienstleistungen, etwa im Rahmen der Steuerverwaltung. Dass damit höhere Kosten als bei der Beauftragung Privater verbunden sind, erscheint zwar nicht unplausibel. Allerdings ist zu berücksichtigen, dass eine unmittelbare Grundrechts- und Gesetzesbindung bei der Erfüllung öffentlicher Aufgaben höhere Anforderungen stellt als das Handeln Privater und deshalb kostenintensiver sein kann. Das Einhalten rechtsstaatlicher Standards kann so zwar höhere Kosten verursachen als ein vergleichbares Handeln Privater, dies ist verfassungsrechtlich aber nicht zu beanstanden, sondern vielmehr hinzunehmende Folge verfassungsrechtlicher Pflichten.

Das Gesetz fordert zusätzlich zu den sonstigen Voraussetzungen einer Auftragsverarbeitung, dass der Zutritt und der Zugang zu den Datenverarbeitungsanlagen, in denen die Akten gespeichert werden, tatsächlich und ausschließlich durch öffentliche Stellen kontrolliert werden. Zwar kann der „Zutritt" nur zu Gebäuden erfolgen, den „Zugang" zu Datenverarbeitungsanlagen wird man aber auf einzelne Arbeitsplätze beziehen müssen.[163] Obwohl es also im Gesetz nicht um den Zugang zu den Daten selbst geht, müsste streng genommen die Nutzung einer Datenverarbeitungsanlage, über die auf die elektronischen Akten zugegriffen werden kann, ausschließlich und tatsächlich durch öffentliche Stellen kontrolliert werden. Gerade das Erfordernis einer tatsächlichen Kontrolle dürfte praktisch kaum zu bewältigende Hürden aufstellen, soweit diese auch effektiv und dem immensen Schutzbedarf der Daten gerecht werden sollen. Ob Formen von Zertifizierungen oder Testaten[164] für eine „tatsächliche" Kontrolle ausreichend sind, ist fraglich. Naheliegender dürfte eine physische Kontrolle sein, gegebenenfalls durchgeführt durch Amtswalter. Will man der staatlichen Gewährleistungsverantwortung nach außen gerecht werden und den notwendigen Schutz der sensiblen personenbezogenen Daten sicherstellen, dürfte diese Regelung einem faktischen Verbot der Einbeziehung Privater gleichkommen. Dass in der Literatur für die Vorschrift noch Überarbeitungsbedarf gesehen wird,[165] erscheint deshalb nachvollziehbar.

Jüngst überarbeitet hat der Gesetzgeber die Regelung zur Verarbeitung von Sozialdaten durch nichtöffentliche Stellen. § 80 Abs. 3 SGB X bestimmt mittlerweile, dass eine Datenverarbeitung durch nichtöffentliche Stellen nur zulässig ist, wenn beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können. Bis zum 24. 5. 2018 fand sich diese Passage in § 80 Abs. 5 SGB X a.F. Nach § 80 Abs. 5 S. 2 SGB X a.F. musste als weitere Voraussetzung für die Datenverarbeitung durch nichtöffentliche Stellen sichergestellt sein, dass der überwiegende Teil der Speicherung des gesamten Datenbestandes beim öffentlichen

[163] Zum Begriff der Datenverarbeitungsanlage, vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 79.

[164] Vgl. *Schrotz/Zdanowiecki*, CR 2015, 485 (488).

[165] *Ritscher*, in: Satzger/Schluckebier/Widmaier (Hrsg.), StPO, § 497 Rn. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Auftraggeber verbleiben musste. Diese letzte Anforderung sollte zwar einem möglichen Herrschafts- und Kontrollverlust entgegentreten,[166] wurde nun aber gleichwohl gestrichen. Sie dürfte sich als nicht praktikabel erwiesen haben. Zum einen sollte sie sich allein auf die Speicherung beziehen, nicht aber andere Formen der Datenverarbeitung.[167] Zum anderen dürfte sich der damit verbundene Eindruck von Sicherheit und Kontrolle in der Realität kaum niedergeschlagen haben. Die Vorstellung, die Kontrolle eines überwiegenden Datenbestands (also effektiv wohl 51 %) würde den spezifischen Gefahren beim Verarbeiten von Daten durch Private vorbeugen, dürfte die Gefahren und das Wesen von Daten nicht hinreichend würdigen. Die Vorschrift veranschaulichte damit die fehlende Abstimmung des gesetzgeberischen Handelns in Bezug auf die Frage der Einbindung privater IT-Dienstleister.

Die jetzige Regelung des § 80 Abs. 3 SGB X verlangt also für eine Auftragsverarbeitung durch Private, dass entweder ansonsten Störungen im Betriebsablauf beim Verantwortlichen auftreten können oder die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können. Der Inhalt der Daten spielt damit für die Frage, ob eine Auftragsverarbeitung zulässig ist, keine Rolle. Sozialdaten können aber von erheblicher Sensibilität für die Betroffenen sein, beispielsweise können auch Gesundheitsdaten i.S.d. Art. 4 Nr. 15 DSGVO erfasst sein. Angesichts dieser Bedeutung ist es nicht nachvollziehbar, dass der Inhalt der Daten keine Bedeutung dafür haben soll, ob diese in den Einflussbereich eines Privaten gelangen und dass hierfür keine Grenzen formuliert werden. Vielmehr zeigt sich, dass gerade im Falle von Sozialdaten der Fokus auf die betriebswirtschaftlichen Erwägungen, der in anderen Referenzgebieten vor allem einen tatsächlichen Beweggrund darstellen mag, im Sozialrecht zur Tatbestandsvoraussetzung erhoben wird. Der Gesetzgeber statuiert damit einen erheblichen Anreiz, kostengünstig Leistungen anzubieten, weil allein das günstigere Leistungsangebot durch einen privaten IT-Unternehmer ausreicht, um die Zulässigkeit der Auftragsverarbeitung tatbestandlich zu begründen. Ein privater IT-Unternehmer hat es durch die möglichst kostengünstige Gestaltung seiner Leistungserbringung selbst in der Hand, ob die Datenübertragung an ihn rechtlich zulässig ist, trotz der möglicherweise sensiblen personenbezogenen Daten, die betroffen sind. Für das notwendige Niveau der Datensicherheit ergibt dies einen bedenklichen Befund.

Auch die Beihilfeakte der Beamtinnen und Beamten enthält sensible personenbezogene Daten, vergleichbar den Sozialdaten. § 108 Abs. 1 S. 3 BBG bestimmt für die Beihilfeakte, dass diese in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Hinter diesem sog. Grundsatz der Abschottung stehen die Vertraulichkeit der Personalakte und Fürsorgepflichten des

[166] *Bieresborn*, in: v. Wulffen/Schütze, SGB X, § 80 Rn. 12a; kritisch dazu *Rammos/Vonhoff*, CR 2013, 265 (267).

[167] *Stähler*, in: Diering/Timme/Stähler (Hrsg.), SGB X, § 80 Rn. 15.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Dienstherrn.[168] Nach § 108 Abs. 5 S. 1 BBG können die Beihilfebearbeitung und die Führung der Beihilfeakte – im Falle des Bundes – lediglich auf eine andere Stelle des Bundes übertragen werden. Eine Übertragung an Private ist nicht zugelassen. Diese Regelung ist, wie auch § 497 StPO und § 80 Abs. 3 SGB X, Ausdruck einer Verpflichtung zum Schutz personenbezogener Daten und damit einer Gewährleistungsverantwortung nach außen.

IV. Vertrauen

Das Vertrauen des Bürgers in den Staat und sein Handeln wird rechtlich typischerweise dann relevant, wenn es als schutzwürdig anerkannt wird.[169] Insofern drückt sich bürgerliches Vertrauen in vielen Facetten aus:[170] Grenzen für rückwirkende Gesetze, beschränkende Regeln für Rücknahme und Widerruf von Verwaltungsakten nach §§ 48, 49 VwVfG, Verbindlichkeit von Zusagen, Fortführung gefestigter Rechtsprechungslinien, aber auch die Annahme, eine Subsidiarität bei der allgemeinen Feststellungsklage gegenüber dem Staat sei unnötig, weil dieser aufgrund des Art. 20 Abs. 3 GG ohnehin Feststellungsurteile umsetzen werde. Viele solcher konkreten Ausprägungen werden auf das Rechtsstaatsprinzip zurückgeführt, aber ein einheitliches rechtliches Modell des Vertrauens sucht man vergeblich.[171]

1. Allgemeine Strukturen des Begriffs „Vertrauen“

Auch der Begriff des Vertrauens lässt sich nicht einheitlich bestimmen; für diesen werden vielmehr je nach wissenschaftlicher Disziplin unterschiedliche Aspekte betont bzw. unterschiedliche Bedeutungen zugrunde gelegt.[172] Verbreitet wird für Vertrauen auf das Einhalten von Erwartungen, das Erfüllen von Vereinbarungen oder ein allgemeines Zutrauen bzw. Sich-Verlassen-Können abgestellt.[173] Es bildet damit

[168] *Hebeler*, in: Battis, BBG, § 108 Rn. 3; *Werres*, ZBR 2001, 429 (435).

[169] Dazu *Schwarz*, Vertrauensschutz als Verfassungsprinzip.

[170] Vgl. allgemein *Eichenhofer*, Der Staat 55 (2016), 41 (52); *H. Huber*, in: Häfelin/Haller/Schindler (Hrsg.), FS Kägi, S. 193 (198).

[171] *Berger*, DVBl. 2017, 804 (805); *Eichenhofer*, Der Staat 55 (2016), 41 (52).

[172] *Möllering*, in: Max-Planck-Institut für Gesellschaftsforschung (Hrsg.), Jahrbuch 2007 – 2008, S. 73 (74), weist auf verschiedene Strömungen in der Psychologie, Soziologie, Politologie, Philosophie und Ökonomie hin. Vgl. außerdem *Baer*, Vertrauen, S. 5; *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 17 (21); *Weilert*, HFR 2010, 207 (208); *H. Huber*, in: Häfelin/Haller/Schindler (Hrsg.), FS Kägi, S. 193 (194 f.). Zur historischen Entwicklung des Vertrauensbegriffs, *Frevert*, in: dies. (Hrsg.), Vertrauen – Historische Annäherungen, S. 7.

[173] *Luhmann*, Vertrauen, S. 1 ff.; *Weilert*, HFR 2010, 207 (208); *Fox*, DuD 2015, 328 (328); *Berger*, DVBl. 2017, 804 (805); *Boehme-Neßler*, MMR 2009, 439 (439); *Baer*, Vertrauen, S. 8 f.; vgl. auch *Grimm/Maier/Rothmund*, DuD 2015, 283; *Baier*, in: Hartmann/Offe (Hrsg.),

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

zwar eine psychologisch-anthropologische Grundlage für das gesellschaftliche Miteinander,[174] ist aber zugleich nicht quantifizierbar, weil es maßgeblich von individuellen Faktoren abhängt.[175] Als Antonyme zum Vertrauen werden Begriffe wie Misstrauen, Argwohn, Unsicherheit oder Zögerlichkeit genannt.[176] Diese Gegenüberstellung verdeutlicht, dass Vertrauen bei einem Zustand zwischen sicherem Wissen und vollständiger Unwissenheit relevant ist.[177] Nach *Kubicek* weist Vertrauen deshalb Ähnlichkeiten zum Glauben auf, denn es „braucht eine Grundlage, ohne vollständig begründbar zu sein".[178]

Vertrauen gewinnt dort an Bedeutung, wo Kontrolle fehlt und Unsicherheit herrscht. Nach *Luhmann* führt Vertrauen in solchen Situationen zur Reduktion der Komplexität, die sich durch ein Defizit an Kontrolle ergibt.[179] Vertrauen bietet damit einen Ausweg für unsichere und undurchschaubare Situationen und schafft Handlungsmöglichkeiten.[180] Ein besonderes Maß an Vertrauen ist deshalb gerade in solchen Bereichen notwendig, die sich neu entwickeln, für den Einzelnen unbekannt sind und für die Erfahrungen fehlen.[181] Auf diesem Wege werden Autonomie gesichert, Persönlichkeitsentfaltung und Aufnahme sozialer Beziehungen ermöglicht und damit die selbstbestimmte Ausübung von Handlungsmöglichkeiten gewährleistet.[182]

Vertrauen weist in erster Linie eine interpersonale Dimension auf, weil Objekt des Vertrauens das Verhalten anderer Menschen ist.[183] Darüber hinaus kann sich Ver-

---

Vertrauen – Die Grundlage des sozialen Zusammenhalts, S. 37; *Oswald*, in: Hof/Kummer/Weingart/Maasen (Hrsg.), Recht und Verhalten, S. 111.

[174] *Boehme-Neßler*, MMR 2009, 439 (439).

[175] *Weilert*, HFR 2010, 207 (208).

[176] *P. Kirchhof*, Recht lässt hoffen, München 2014, S. 91.

[177] *Simmel*, Gesamtausgabe XI, Soziologie, S. 302; *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 17 (23); *Griesser/Buntschu*, DuD 2016, 640 (641).

[178] *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 17 (23).

[179] *Luhmann*, Vertrauen, S. 27 ff. Nach *Luhmann* kann ein Vertrauensverhältnis in sachlicher Hinsicht zur Reduktion von Komplexität, in sozialer Hinsicht für stabile soziale Interaktionen und in zeitlicher Hinsicht für die Fortdauer von solchen Beziehungen Bedeutung aufweisen. Vgl. *Schaal*, Vertrauen, Verfassung und Demokratie, S. 64; *Boehme-Neßler*, MMR 2009, 439 (439); *Eichenhofer*, Der Staat 55 (2016), 41 (51); *Fox*, DuD 2015, 328 (328); *Griesser/Buntschu*, DuD 2016, 640 (641).

[180] *Boehme-Neßler*, MMR 2009, 439 (439).

[181] *Vassilaki*, CR 2002, 742 (743).

[182] *Eichenhofer*, Der Staat 55 (2016), 41 (50); *Boehme-Neßler*, MMR 2009, 439 (439 f.).

[183] *Schaal*, Vertrauen, Verfassung und Demokratie, S. 31; *Fox*, DuD 2015, 328 (328); *Oswald*, in: Hof/Kummer/Weingart/Maasen (Hrsg.), Recht und Verhalten, Baden-Baden 1994, S. 116 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

trauen aber auch auf ein System oder eine Institution beziehen.[184] Auch diesen gegenüber können bestimmte Erwartungen bestehen. Für denjenigen, in den Vertrauen gesetzt wird, kann Vertrauen deshalb einen gewissen Druck erzeugen, entgegengebrachtes Vertrauen nicht zu enttäuschen.[185] Denn Vertrauen kann schnell schwinden und einen langfristigen (Wieder-)Aufbau bzw. aufwendige wiederkehrende Bestätigung erfordern.[186]

2. Generell: Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen

Das Vertrauen Einzelner in konkrete Handlungen und Verhaltensweisen des Staates kann unter bestimmten Umständen rechtliche Bedeutung erlangen, wie die eingangs geschilderten Anwendungsfälle deutlich machen. Über solche Einzelfälle hinaus kann ein allgemeines Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen als zwingende Voraussetzung für den demokratischen Rechtsstaat angesehen werden.[187] Treffend hat dies *Ernst Benda* unter dem Eindruck des technischen Wandels der 80er Jahre klargestellt: „Der Staat ist auf das Vertrauen seiner Bürger angewiesen, und er ist verpflichtet, sich hierum nach Kräften zu bemühen."[188]

Ideengeschichtlich lässt sich diese Prämisse auf Überlegungen von *John Locke* zurückführen.[189] Nach seiner Annahme schließen die Menschen einen Gesellschaftsvertrag, der eine Übertragung der individuellen Rechte auf einen Souverän bewirkt.[190] Hintergrund dieses Gesellschaftsvertrags sind für *Locke* die Verteilungskonflikte, die sich im hypothetischen Naturzustand, in dem alle Menschen durch vollkommene Freiheit und Gleichheit gekennzeichnet sind, durch das Schaffen von Eigentum und die Vergesellschaftung ergeben.[191] Diese Übertragung von indi-

[184] *Schaal*, Vertrauen, Verfassung und Demokratie, S. 52; *Boehme-Neßler*, MMR 2009, 439 (440); a.A. *Eichenhofer*, Der Staat 55 (2016), 41 (53). Vgl. *Grimm/Maier/Rothmund*, DuD 2015, 283, die ein Modell gerade für institutionelles Vertrauen darstellen.

[185] *Fox*, DuD 2015, 328 (328).

[186] *Kuhlen*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 37 (39).

[187] *P. Kirchhof*, Recht lässt hoffen, S. 91 ff.; *Weilert*, HFR 2010, 207 (207 ff.); *Maurer*, in: Isensee/P. Kirchhof (Hrsg.), HStR IV, § 79, Rn. 11; *Schwarz*, Vertrauensschutz als Verfassungsprinzip, S. 43; *Schaal*, Vertrauen, Verfassung und Demokratie, S. 11, 189; vgl. *Ossenbühl*, DÖV 1972, 25 (25).

[188] *Benda*, DuD 1984, 86 (87).

[189] Vgl. *Schaal*, Vertrauen, Verfassung und Demokratie, S. 67 ff.; *H. Huber*, in: Häfelin/Haller/Schindler (Hrsg.), FS Kägi, S. 193 (193 f.).

[190] *Locke*, Zwei Abhandlungen über die Regierung, II § 95.

[191] *Locke*, Zwei Abhandlungen über die Regierung, II §§ 4, 123.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

viduellen Rechten durch einen Gesellschaftsvertrag dient dem Ziel, Frieden, Sicherheit und das öffentliche Wohl zu gewährleisten.[192] Das Eingehen dieses Gesellschaftsvertrags ist nach *Locke* untrennbar mit dem Vertrauen verbunden, dass der Souverän die in ihn gesetzten Erwartungen erfüllt.

> „Denn da alle *Gewalt, die im Vertrauen auf einen bestimmten Zweck übertragen wird*, durch diesen Zweck begrenzt ist, so muss, wenn dieser *Zweck* vernachlässigt oder ihm entgegen gehandelt wird, dieses *Vertrauen* notwendigerweise *verwirkt* sein und die Gewalt in die Hände derjenigen zurückfallen, die sie erteilt haben und die sie nun von neuem vergeben können, wie sie es für ihre Sicherheit und ihren Schutz am besten halten können."[193]

Zum Teil wird sogar davon ausgegangen, dass sich nach *Locke* die Legitimität einer Regierung nicht durch den Wahlakt ergibt, sondern auf deren vertrauenswürdigem Handeln beruht.[194]

Hinter diesem Konzept von Vertrauen in den Staat und sein Handeln steht auch das traditionelle Über-/Unterordnungsverhältnis, das für das Zusammenspiel von Staat und Bürgern seit jeher in weiten Bereichen prägend ist.[195] Der Einzelne unterwirft sich der Überordnung des Staates, weil er darauf vertraut, dass dieser seine Interessen und Güter wahrt. Die Aufrechterhaltung dieses Verhältnisses erfordert ebenfalls ein hinreichendes Maß an Vertrauen.

Im modernen Rechtsstaat wird dieses Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen durch umfangreiche Kontrollmechanismen gegen einen Missbrauch unterstützt.[196] Für den Bürger folgen daraus in erster Linie die verwaltungs- und verfassungsprozessual vorgesehenen Rechtsmittel bis hin zur Verfassungsbeschwerde.[197] Dabei erstreckt sich das Vertrauen auch auf das Funktionieren der Kontrollmechanismen selbst. Was diesen Aspekt des Vertrauens in den Staat und sein Handeln angeht, kommt dem Recht eine überragende Bedeutung zu, nicht nur für das Funktionieren der prozessualen Mittel, sondern insbesondere auch für die zugrundeliegenden subjektiven öffentlichen Rechtspositionen. Das Bilden und Erhalten von Vertrauen und das Schaffen von Erwartungssicherheit werden damit zu Aufgaben des Rechts.[198] Indem rechtliche Regelungen den Staatsorganen und deren Handeln Legitimität verleihen, wird Vertrauen be-

---

[192] *Locke*, Zwei Abhandlungen über die Regierung, II § 131.

[193] *Locke*, Zwei Abhandlungen über die Regierung, II § 149 (Hervorh. im Original).

[194] *Schaal*, Vertrauen, Verfassung und Demokratie, S. 71.

[195] *Weilert*, HFR 2010, 207 (219).

[196] *Weilert*, HFR 2010, 207 (207, 214 ff.); vgl. *Baer*, Vertrauen, S. 9. Vgl. auch BVerfGE 123, 39 (69); EuGH, Urt. v. 6.10.2015, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650, Rn. 81.

[197] Vgl. *Weilert*, HFR 2010, 207 (214 f., 217), die auch für das Verhältnis der Staatsorgane zueinander auf den Grundsatz der Gewaltenteilung und die damit im Zusammenhang stehenden verfassungsrechtlichen Kontrollmechanismen verweist.

[198] *Boehme-Neßler*, MMR 2009, 439 (439).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

gründet.[199] Dabei hat die konkrete Ausgestaltung solcher rechtlichen Kontrollmechanismen das Spannungsverhältnis von Vertrauen und Misstrauen sowie die tatsächlichen Gegebenheiten zu berücksichtigen.[200]

Das Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen mündet vorrangig in der Erwartung, konkrete Rechtspositionen würden gewahrt werden. Dies kann etwa zu einem Vertrauen auf die sichere Betätigung grundrechtlicher Freiheiten und der Erwartung eines ausreichenden Schutzes persönlicher Daten führen.[201] Darüber hinaus kann auf die oben dargestellten Regelungen für die Einbindung privater IT-Dienstleister verwiesen werden, etwa auch die Funktionsfähigkeit der Verwaltung und eine darauf gerichtete Gewährleistungsverantwortung nach innen. Schon diese Bezugnahme macht jedoch deutlich, dass Vertrauen des Einzelnen in den Staat nicht auf subjektive Rechte des Einzelnen gegenüber dem Staat beschränkt werden kann. In der Tradition *John Lockes* entwickelt Vertrauen darüber hinaus eine eigenständige Bedeutung, die eine Art Metaebene berührt.[202] Losgelöst von der Einhaltung konkreter rechtlicher Regeln kann Vertrauen gegenüber dem Staat ein Wert an sich sein. So lässt sich ein Vertrauen in die Richtigkeit des vom Staat erlassenen Rechts konturieren.[203] Damit im Zusammenhang kann sich Vertrauen auch darauf erstrecken, dass der Staat eine gerechte Ordnung errichtet und staatliches Handeln am Allgemeinwohl ausgerichtet ist.[204] Schließlich besteht ein Vertrauen in die Funktionsfähigkeit der Verwaltung als Grundelement der Ausübung von Staatlichkeit.

3. Speziell: Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien

Das Vertrauen gegenüber dem Einsatz digitaler Informationstechnologien durch den Staat und insbesondere einem Transfer von staatlichen Daten, der dazu führt, dass diese zumindest mittelbar Einflussmöglichkeiten von Privaten ausgesetzt sind, ist durch besondere Strukturen gekennzeichnet.

a) Zuspitzung durch gegensätzliche Entwicklungen

Im Ausgangspunkt ist das Vertrauen in diese Form staatlichen Handelns durch zwei gegensätzliche Entwicklungskräfte gekennzeichnet: einerseits die Notwen-

[199] *Weilert*, HFR 2010, 207 (207).

[200] *Boehme-Neßler*, MMR 2009, 439 (440).

[201] Vgl. *Weilert*, HFR 2010, 207 (228).

[202] Wohl a.A. *Eichenhofer*, Der Staat 55 (2016), 41 (52); *Weilert*, HFR 2010, 207 (219).

[203] *P. Kirchhof*, Recht lässt hoffen, München 2014, S. 109 ff.; *H. Huber*, in: Häfelin/Haller/Schindler (Hrsg.), FS Kägi, S. 193 (193).

[204] Vgl. *Weilert*, HFR 2010, 207 (219 f.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

digkeit eines erhöhten Maßes an Vertrauen aufgrund des Einsatzes relativ neu entstandener und ungewohnter Techniken und andererseits den Verlust herkömmlicher Kontrollmechanismen.

aa) Besonderes Bedürfnis nach Vertrauen bei neuartigen Herausforderungen – Einsatz digitaler Informationstechnologien

Die staatliche Verwaltung arbeitet seit jeher mit der traditionellen Schriftform und körperlichen Akten. In den letzten drei Jahrzehnten allerdings haben sich digitale Informationstechnologien mit erheblicher Macht ihren Weg gebahnt, auch in der Verwaltung. Diese befindet sich derzeit in einer Phase des Umbruchs, in der digitale und herkömmliche Prozesse nebeneinanderstehen. Für manche ist dieses Nebeneinander Anlass, darauf hinzuweisen, dass das Vertrauen in Handlungen, Entscheidungen und Verfahren, die maßgeblich oder ausschließlich virtuell stattfinden, ebenso wichtig sei wie das Vertrauen in Handlungen, die körperlich-gegenständlich erfolgen.[205] Noch überzeugender dürfte jedoch die Annahme sein, dass das Vertrauen in digitale Informationstechnologien sogar erheblich bedeutender ist.[206]

Vertrauen wird dann besonders wichtig, wenn das Objekt des Vertrauens noch nicht auf eine weitreichende Historie verweisen kann, sondern sich gerade erst entwickelt oder entstanden ist.[207] Deutlich wird dies, wenn man Vertrauen auf die drei Elemente Vernunft, Routine und Erfahrungen zurückführt.[208] Schlicht an Routine und insbesondere Erfahrung mangelt es bislang beim Einsatz digitaler Informationstechnologien durch Träger staatlicher Gewalt, jedenfalls im Vergleich zur traditionellen Schriftform und dem Führen körperlicher Akten. Gerade angesichts des dadurch ausgelösten Umbruchs in der öffentlichen Verwaltung und bei der sonstigen Wahrnehmung öffentlicher Aufgaben kommt dem Vertrauen in diese Prozesse eine erhebliche Bedeutung zu. Nur auf diesem Wege gelingt es, Akzeptanz für diesen Umbruch zu erzeugen.[209]

Nur durch ein ausreichendes Maß an Vertrauen bleiben individuelle Handlungsmöglichkeiten bestehen, Autonomie gewährleistet und Freiheiten gesichert.[210] Sobald der Bürger in der Unsicherheit lebt, dass er nicht weiß, was mit den Daten, die

[205] *Boehme-Neßler*, MMR 2009, 439 (439).

[206] In diese Richtung *Grimm/Maier/Rothmund*, DuD 2015, 283 (283); *Weichert*, GesR 2005, 151 (152); *Heckmann*, K&R 2010, 1 (6). Zur Bedeutung des Datenschutzes für das Vertrauen in den Staat *Meyer-Ladewig/Nettesheim*, in: dies./von Raumer (Hrsg.), EMRK, Art. 8 Rn. 32; zu diesbezüglichen Ansätzen in der Rechtsprechung des EuGH *Eichenhofer*, Der Staat 55 (2016), 41 (66).

[207] *Vassilaki*, CR 2002, 742 (743).

[208] So *Möllering*, in: Max-Planck-Institut für Gesellschaftsforschung (Hrsg.), Jahrbuch 2007 – 2008, S. 73 (74 f.).

[209] Vgl. *Berger*, DVBl. 2017, 804 (805); *Heckmann*, K&R 2010, 1 (6).

[210] Vgl. *Boehme-Neßler*, MMR 2009, 439 (439 f.).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

er dem Staat überlässt, geschieht und welche Entwicklung sie durchlaufen werden, kann dies stets zu einem Hindernis für Interaktion mit dem Staat werden.[211]

Bislang wurzelte das Vertrauen, das Trägern öffentlicher Gewalt entgegengebracht wurde, in erster Linie in der Person des einzelnen Amtswalters. Dieser persönliche Aspekt, der z. B. in den Prinzipien kommunaler Selbstverwaltung prägend zum Tragen kommt,[212] wird durch den Einsatz digitaler Informationstechnologien mehr und mehr in den Hintergrund gedrängt. Für die Strukturen der Vertrauensbildung kommt es zu tiefgreifenden Umwälzungen. Zunehmend geht es nicht mehr darum, in Personen zu vertrauen, sondern in die Richtigkeit digitaler Prozesse.[213] Kommt es insofern zu einem Vertrauensverlust, kann dies Funktionsstörungen hervorrufen, deren Auswirkungen mehr als nur das individuelle Verhältnis zum einzelnen Bürger betreffen.[214] In dem Fall steht die Nutzbarkeit der Informationstechnologie selbst auf dem Spiel. Die Bedeutung des Vertrauens hat sich deshalb immens gesteigert.

bb) Auflösung gängiger Kontrollstrukturen

Vertrauen wird typischerweise durch Kontrollmechanismen begleitet. Dabei ist die tatsächliche Wahrnehmung stets der vorrangige Anknüpfungspunkt für Kontrollmechanismen. So ist staatliches Handeln in erster Linie deshalb kontrollierbar, weil es sich grundsätzlich unmittelbar in der tatsächlichen oder rechtlichen Ordnung auswirkt und als solches auch unmittelbar wahrnehmbar ist. Für die Handhabung mit Daten stoßen solche Kontrollmechanismen aber (zumindest bislang) an ihre Grenzen.[215]

Das Erheben, Nutzen und Verarbeiten von Daten durch Speichern, Verändern, Übermitteln oder Löschen ist regelmäßig der unmittelbaren menschlichen Wahrnehmung entzogen. Ob etwa Daten unberechtigterweise weitergegeben werden und von Dritten unberechtigt genutzt werden, ist für den Betroffenen regelmäßig nicht wahrnehmbar, insbesondere wenn dies lediglich zu einer Wissenserweiterung bei Dritten führt. Ob Daten korrumpiert werden und inhaltlich unrichtig sind, wird häufig nicht ohne weiteres wahrnehmbar sein, insbesondere wenn Betroffene nur das Ergebnis einer Datenverarbeitung erfahren und lediglich unter erschwerten Umständen den Entscheidungsfindungsprozess konkret rekonstruieren können. Ob Daten unberechtigterweise allgemein zugänglich gemacht werden, wird der Betroffene zwar grundsätzlich wahrnehmen können, doch in dem Fall lässt sich die

[211] *Benda*, DuD 1984, 86 (87); vgl. BVerfGE 65, 1 (43).

[212] Vgl. *Vogelgesang/Lübking/Ulbrich*, Kommunale Selbstverwaltung, Rn. 23.

[213] *Berger*, DVBl. 2017, 804 (805); vgl. *Kuhlen*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 37 (41); *Kaiser*, Die Kommunikation der Verwaltung, S. 111 ff.

[214] *Hoffmann-Riem*, AöR 134, 513 (535); *Weichert*, GesR 2005, 151 (152).

[215] Vgl. BVerfGE 125, 260 (322 f.); *Benda*, DuD 1984, 86 (87).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Verbreitung tatsächlich regelmäßig nicht mehr rückgängig machen.[216] Für den Umgang mit Daten muss deshalb aus faktischen Gründen eine wesentlich geringer entwickelte und weniger leistungsfähige Instrumentalisierung möglichen Misstrauens konstatiert werden. Befördert wird diese Entwicklung durch einen komplizierten rechtlichen Rahmen und die Ubiquität, Anonymität und Globalisierung im Bereich digitaler Informationstechnologien.[217] Dem Einsatz digitaler Informationstechnologien haftet im Ergebnis eine grundsätzliche Undurchschaubarkeit an, die weniger effektive Kontrollmechanismen bedingt.[218]

Vertrauen wird aber umso wichtiger, je geringer die Kontrollmöglichkeiten ausgeprägt sind. Diese Herausforderung ist generell mit virtuellen Räumen verbunden.[219] Zwar ist ein Vertrauen in den Einsatz digitaler Informationstechnologien auch unter diesen Vorzeichen prinzipiell möglich, es unterliegt aber erheblich erschwerten Bedingungen und ist erheblich leichter zu erschüttern. Dem Recht als Faktor zur Bildung von Vertrauen kommt deshalb eine gesteigerte Bedeutung zu.

b) Konsequenzen für die rechtlichen Grundlagen der Vertrauensbildung

Welche Folgerungen lassen sich nun vor dem Hintergrund dieser gegensätzlichen Entwicklungskräfte – einerseits ein erhöhter Bedarf an Vertrauen, andererseits der Verlust gängiger Kontrollstrukturen – für die Aufgabe des Rechts, Vertrauen zu schaffen und zu erhalten, ableiten?

Zum Teil wird angenommen, für den Schutz des Vertrauens im virtuellen Raum sei zukünftig der Bürger selbst zuständig.[220] Für den Schutz von Persönlichkeitsrechten gegenüber anderen Privaten kann dem eigenen Verhalten tatsächlich eine wesentliche Rolle zukommen,[221] wobei man selbst in solchen Konstellationen nicht davon ausgehen darf, dass dies den Staat von seinen Aufgaben – etwa aufgrund grundrechtlicher Schutzpflichten – entbinden würde. Im Verhältnis zum Staat ergibt sich im Übrigen ein anderes Bild: Der staatliche Umgang mit Daten richtet sich typischerweise nach gesetzlichen Regelungen. Dem Bürger ist dabei grundsätzlich kein Spielraum überlassen, der zum Schutz des Vertrauens selbständig genutzt

[216] Vgl. oben C. III. 2. a) (2).

[217] *Gaycken*, DuD 2011, 346 (346 f.).

[218] *Eichenhofer*, Der Staat 55 (2016), 41 (51); *Boehme-Neßler*, MMR 2009, 439 (441); *Heckmann*, K&R 2010, 1 (7); *Gaycken*, DuD 2011, 346 (346).

[219] Vgl. *Kuhlen*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 37 (37 f.); *Roßnagel/Richter/Nebel*, in: Buchmann (Hrsg.), Internet Privacy, S. 281 (282).

[220] *Boehme-Neßler*, MMR 2009, 439 (442).

[221] Tatsächlich dürfte auch für den Einzelnen eine hinreichende informationelle Selbstbestimmung immer weniger über sicheres Wissen zu erreichen sein, *Gaycken*, DuD 2011, 346 (346). Nach *Eichenhofer*, Der Staat 55 (2016), 41 (50 f.) kann hingegen Vertrauen die Grundlage einer Neukonzeption des Schutzes von Privatheit im Internet bilden.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

werden könnte. Im Zweifel ist eigeninitiatives Handeln zum Selbstschutz rechtswidrig. Zwar ist nicht ausgeschlossen, dass auch Zertifizierungen, Empfehlungen oder Reputationsdienste eine gewisse vertrauensbildende Wirkung erzeugen können, wenn sie Träger staatlicher Gewalt zum Gegenstand haben, doch dürften diese Wirkungen gering bleiben, weil zur staatlichen Tätigkeit keine Alternative verfügbar ist. Stattdessen bedarf es anderer Mechanismen.

aa) Erheblich gesteigerte Bedeutung des Vertrauens in den staatlichen Einsatz digitaler Informationstechnologien

Das Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen mag zwar ohne ausdrückliche geschriebene rechtliche Verankerung auskommen, gleichwohl handelt es sich um eine unabdingbare Voraussetzung staatlichen Wirkens. Dies gilt umso mehr für den staatlichen Einsatz digitaler Informationstechnologien. Der Grundsatz digitaler Souveränität ist in dieser Hinsicht Ausdruck von Staatlichkeit. Dies ergibt sich schon deshalb, weil bei einer realistischen Betrachtung ein Funktionsverlust dieser Systeme die ernsthafte Gefahr eines Zusammenbruchs staatlicher Funktionen begründet.

Deren Funktionsfähigkeit setzt weiter die Bereitschaft der Bürger voraus, solchen Technologien zu vertrauen. Fehlt es an der bürgerlichen Akzeptanz, kann der staatliche Einsatz von Informationstechnologien nicht die Effektivität und Effizienz erreichen, die zur Aufrechterhaltung der Verwaltungsfunktion notwendig ist. Ein seit jeher bestehendes Vertrauen in die Rechtmäßigkeit von staatlichen Entscheidungen erweitert sich aufgrund der tatsächlichen Bedeutung von Daten und digitalen Informationstechnologien zum Vertrauen in die Integrität staatlicher Daten als essenzielle Grundlage staatlicher Entscheidungen. Notwendig ist deshalb auch das Vertrauen in die inhaltliche Richtigkeit der verwendeten Daten.

Das Vertrauen muss sich weiter darauf erstrecken, dass für personenbezogene Daten das notwendige Maß an Vertraulichkeit gesichert ist und diese nicht von Dritten sachfremd verwendet oder gar veröffentlicht werden. Zwar hat das Bundesverfassungsgericht für das jüngst entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme festgestellt, dass dieses nur solche Systeme erfasst, die als eigene genutzt werden.[222] Das Grundrecht erstreckt sich also nicht auf personenbezogene Daten, die in staatlichen Systemen vorhanden sind. Allerdings ist es möglich, dass Bürger personenbezogene Daten lediglich aufgrund eines Unter-/Überordnungsverhältnisses zum Staat Preis gegeben haben und sie deshalb die Erwartung haben, dass diese weitreichenden hoheitlichen Befugnisse auch mit einer besonderen Verantwortung einhergehen. Auch insoweit besteht also ein begründetes besonderes Vertrauen.

[222] BVerfGE 120, 274 (315); dazu *Hornung*, CR 2008, 299 (303).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

bb) Schwelle zwischen öffentlich-rechtlichem und privatrechtlichem Bereich

Diese erheblich gesteigerte Bedeutung des Vertrauens in den Einsatz digitaler Informationstechnologien bezieht sich auf die beteiligten Personen bzw. Organisationen. Für einen strukturellen Vergleich des Maßes an Vertrauen, das einerseits Akteuren im IT-Bereich entgegengebracht werden kann, die von der öffentlichen Hand betrieben werden, und andererseits solchen, die sich in privater Hand befinden, sind die prozessualen und materiell-rechtlichen Kontrollmechanismen zu berücksichtigen. Das Recht ist wie erörtert ein maßgeblicher Faktor für die Vertrauensbildung. Sowohl in diesem Sinne öffentlich-rechtliche wie auch private Akteure mögen zwar Ziele haben, die den Interessen individuell Betroffener widerstreiten. Doch sind Akteure, die von der öffentlichen Hand betrieben werden, dabei unmittelbar an die Grundrechte gebunden[223] und unterliegen einfachgesetzlichen Verpflichtungen. Träger staatlicher Gewalt verfügen zwar über verbindliche Eingriffsbefugnisse, unterliegen überdies aber auch dem Vorrang und Vorbehalt des Gesetzes und sind verschiedensten subjektiven öffentlichen Rechten verpflichtet. Sie agieren neutral und verfolgen öffentliche Aufgaben, die das Gemeinwohl berücksichtigen. Für Träger staatlicher Gewalt hat die Aufrechterhaltung eines funktionsfähigen Gemeinwesens eine grundsätzlich andere Bedeutung als für private Akteure.

IT-Dienstleister hingegen, die sich in privater Hand befinden, sind allenfalls mittelbar an die Grundrechte gebunden, können privatautonom gesteckte Ziele verfolgen und aus Eigennutz handeln.[224] Welchem (nationalen) Regelungsregime sie bzw. die Daten, die sich in ihrem Hoheitsbereich befinden, unterfallen, kann unklar sein und sich im Laufe von Geschäftsbeziehungen ändern. Aufgrund dieser Wesensunterschiede ist das Vertrauen bei objektiver Betrachtung gegenüber Akteuren in öffentlich-rechtlicher Hand strukturell ausgeprägter; anders gewendet ist gegenüber privaten IT-Dienstleistern ein größeres Vertrauen erforderlich.[225] Vertrauen in private IT-Dienstleister wird aber in regelmäßigen Abständen immer wieder massiv erschüttert. Anschaulich zeigte dies der Rechtsstreit um einen Zugriff US-amerikanischer Regierungs- und Justizbehörden auf Daten, die vom US-amerikanischen Unternehmen Microsoft in Drittstaaten verwaltet werden. Auch wenn dieses Verfahren vor dem U.S. Supreme Court mittlerweile von den Parteien wegen einer Gesetzesänderung für erledigt erklärt wurde, setzt sich der eigentliche Streit unter anderen gesetzlichen Vorzeichen fort. Schon dieses über Jahre andauernde und nach wie vor bestehende Herausgabeverlangen der Behörden und die Diskussion darüber lässt das Vertrauen in solche privaten IT-Dienstleister erheblich sinken.

Durch eine Begrenzung auf IT-Dienstleister, die von der öffentlichen Hand betrieben werden, kann dem Gebot der Verantwortungsklarheit Geltung verschafft

[223] Vgl. BVerfGE 128, 226 (245).

[224] Vgl. *Vassilaki*, CR 2002, 742 (743 f.).

[225] *Griesser/Buntschu*, DuD 2016, 640 (645).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

werden.[226] Ein vertrauensvoller Umgang mit Daten ist nur dann möglich, wenn von vornherein und eindeutig klar ist, dass diese in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben, der durch unmittelbare Grundrechts- und Gesetzesbindung gekennzeichnet ist, und sichergestellt ist, dass die Daten nicht einem privaten Herrschaftsbereich ausgesetzt sind, in dem Eigeninteressen und privatautonome Dispositionsbefugnis die grundsätzlichen Leitmotive bilden.

cc) Ersetzen von Mechanismen zur Missbrauchskontrolle durch Handlungsgrenzen

Prinzipiell können sich Kontrollmechanismen, die die Vertrauensbildung unterstützen, darauf beschränken, mögliches Fehlverhalten abzuwarten und im Nachhinein korrigierend einzugreifen, sobald das Fehlverhalten erkennbar geworden ist. Kontrollmechanismen stehen aber dem Problem gegenüber, dass Fehlverhalten, das Daten betrifft, nur schwer zu identifizieren und rückgängig zu machen ist.[227] Das mögliche Misstrauen, das dem Einsatz digitaler Informationstechnologien entgegengebracht wird, ist deshalb aufgrund der tatsächlichen Gegebenheiten nicht in einer Art und Weise (rechtlich) instrumentalisiert, die effektiv ist. Insbesondere erscheinen staatliche Schutzpflichten aufgrund ihrer Unbestimmtheit nicht ausreichend geeignet, einem möglichen Misstrauen entgegenzuwirken.[228]

Rechtliche Strukturen zur Vertrauensbildung beim staatlichen Umgang mit Daten müssen deshalb an einer vorgelagerten Stufe ansetzen. Da tatsächliche Kontroll- und Korrekturmöglichkeiten in weiten Teilen fehlen, ist es notwendig, gar nicht erst zuzulassen, dass Daten den öffentlich-rechtlich geprägten Herrschaftsbereich verlassen. Vertrauen knüpft an eine Form der Integrität von Daten an, die durch das gängige Modell der nachträglichen Missbrauchskontrolle schon in Frage gestellt wäre – ein fehlerhafter Umgang mit Daten ist eben häufig nicht wahrnehmbar oder rückgängig zu machen. Für diese Facette des Grundsatzes digitaler Souveränität kommt es darauf an, ob die wahrgenommene Aufgabe typisch für die Ausübung von hoheitlichen Befugnissen ist. Dies knüpft an die ideengeschichtliche Verbindung von Vertrauen und Staatlichkeit an und kann zu Überschneidungen mit obligatorischen Staatsaufgaben und deren integralen Bestandteilen führen. Außerdem greift der Grundsatz digitaler Souveränität hier umso eher ein, je mehr der Staat für die reibungslose und effektive Aufgabenerfüllung darauf angewiesen ist, dass ihm die Bürger vertrauen und an der Aufgabenerfüllung einvernehmlich mitwirken, und je weniger dieser Aspekt des einvernehmlichen Mitwirkens durch hoheitliche Befugnisse und Kontrollmöglichkeiten in praktikabler Weise ersetzt werden könnte.

Ein so verstandener Schutz von Vertrauen in den staatlichen Umgang mit Daten ist in die Zukunft gerichtet und kann seine Wirkung gerade in Zeiten entfalten, in denen

[226] Vgl. *Berger*, DVBl. 2017, 804 (806).

[227] Vgl. oben C. III. 2. a) bb).

[228] Vgl. oben C. III. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

es an Erfahrung und Routine mangelt. Das notwendige Maß an Verlässlichkeit und Verantwortlichkeit wird durch eine in ihrer Folge klare Regelung ermöglicht, wonach bestimmte Daten bei einem Akteur zu verbleiben haben, der von der öffentlichen Hand betrieben wird.[229] Dies bewirkt die notwendige Entlastung der Bürger, die darauf vertrauen können, dass ihre Daten, die von einem Träger staatlicher Gewalt verwendet werden, auch in der staatlichen Sphäre verbleiben und nicht in den Herrschaftsbereich privater Dritter gelangen.

Für diese Vorverlagerung der Kontrollstrukturen spricht auch, dass beeinträchtigtes Vertrauen häufig lange Zeit und umfangreiche Bemühungen braucht, um wieder aufgebaut zu werden.[230] Bei einem Vertrauensverlust gegenüber dem Staat steht aber kein Markt zur Verfügung, auf dem sich (noch) vertrauenswürdige Ersatzakteure befinden, die an die Stelle des Staates treten könnten.[231] Auch wenn die öffentlich-rechtliche Ebene durch eine Vielzahl von Trägern staatlicher Gewalt stark fragmentiert ist, wird dennoch der Staat als einheitliches Gebilde wahrgenommen. Dieser Staat und das in ihn gesetzte Vertrauen sind singulär und deshalb in höchstem Maße schutzwürdig.

4. Beispiele: Finanzverwaltung, §§ 2 Abs. 2, 17 Abs. 3, 20 FVG, und Registerwesen, § 126 Abs. 3 GBO, § 387 Abs. 5 FamFG

Das Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien wird sich häufig auf die Entscheidung über obligatorische Staatsaufgaben, deren integrale Bestandteile oder das Maß der Gewährleistungsverantwortung auswirken. Darüber hinaus kann es jedoch auch als eigenständiger Begründungsansatz für einen Grundsatz digitaler Souveränität in Betracht kommen und zwar beispielhaft im Bereich des Steuergeheimnisses und des Registerwesens.

Die Finanzverwaltung war seit jeher einer der maßgeblichen Wegbereiter beim Einsatz von Informationstechnologien in der öffentlichen Verwaltung.[232] Ihre Verwendung und auch ihre institutionelle Einbindung ist daher vergleichsweise umfangreich gesetzlich geregelt. § 17 Abs. 3 FVG hat den Einsatz automatisierter Datenverarbeitungssysteme mit Entscheidungscharakter zum Gegenstand. Die Regelung ermöglicht, falls im Besteuerungsverfahren automatische Einrichtungen eingesetzt werden, dass damit zusammenhängende Steuerverwaltungstätigkeiten

[229] Vgl. *Weilert*, HFR 2010, 207 (222).

[230] Vgl. *Kuhlen*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 37 (39).

[231] Zwar existieren eine Vielzahl von Trägern staatlicher Gewalt, doch hat der Einzelne aufgrund der gesetzlichen Zuständigkeitsordnung grundsätzlich keine freie Wahl zwischen diesen.

[232] §§ 17 Abs. 3, 2 Abs. 2 FVG wurden schon durch das Steuerbereinigungsgesetz vom 14. 12. 1984 in das FVG eingefügt, BGBl. I S. 1493.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

durch Rechtsverordnung der zuständigen Landesregierung auf ein nach § 2 Abs. 2 FVG eingerichtetes Rechenzentrum übertragen werden können. Dort ist vorgesehen, dass Rechenzentren der Landesfinanzverwaltung als Teil der für die Finanzverwaltung zuständigen obersten Landesbehörde, als Oberbehörde oder als Teil einer näher bestimmten Oberbehörde, als Teil einer Oberfinanzdirektion, als Finanzamt oder als Teil eines Finanzamtes eingerichtet werden können. In jedem Fall muss das Rechenzentrum institutioneller Teil der öffentlichen Finanzverwaltung sein. Damit wird dem Gebot der obligatorischen Finanzverwaltung Rechnung getragen, das sich aus Art. 108 Abs. 1, 2 GG ergibt.[233]

Daneben regelt § 20 FVG den Einsatz automatischer Einrichtungen, soweit diese nur mechanische Hilfstätigkeiten ausüben.[234] Nach § 20 Abs. 1 FVG liegt die Entscheidung über den Einsatz automatischer Einrichtungen bei der jeweiligen obersten Landesbehörde. Dabei kann auch vorgesehen werden, dass solche Systeme anderer Träger verwendet werden, allerdings nur, soweit diese von Finanzbehörden des Bundes, eines anderen Landes oder anderer Verwaltungsträger getragen werden. Auch im Anwendungsbereich des § 20 Abs. 1 FVG ist die Übertragung der Datenverarbeitung auf private IT-Dienstleister nicht zulässig.

Diese Vorschriften führen dazu, dass Daten der Finanzverwaltung in einem ausschließlich öffentlich-rechtlich geprägten Einflussbereich verbleiben und flankieren so in institutionell-organisatorischer Hinsicht das Steuergeheimnis des § 30 AO. Unter Berücksichtigung des Charakters des Steuergeheimnisses lassen sich deshalb die Gründe für die zwingende Datenverarbeitung durch Träger staatlicher Gewalt identifizieren. Vordergründig scheint sich dabei vor allem das Recht auf informationelle Selbstbestimmung der Steuerpflichtigen auszuwirken.[235] Dies lässt den gesetzlichen Vorbehalt für öffentliche IT-Dienstleister auf Grundlage des Steuergeheimnisses als Konsequenz einer Gewährleistungsverantwortung nach außen erscheinen. Das Bundesverfassungsgericht hat jedoch hervorgehoben, dass die Bedeutung des Steuergeheimnisses über die individuelle Rechtsposition der jeweiligen Steuerpflichtigen hinausgeht.

> „Sie [scil. die Vorschrift des § 30 AO] dient zum einen dem privaten Geheimhaltungsinteresse des Steuerpflichtigen und der anderen zur Auskunftserteilung verpflichteten Personen. Zugleich wird mit ihr der Zweck verfolgt, durch besonderen Schutz des Vertrauens in die Amtsverschwiegenheit die Bereitschaft zur Offenlegung der steuerlich relevanten Sachverhalte zu fördern, um so das Steuerverfahren zu erleichtern, die Steuerquellen vollständig zu erfassen und eine gesetzmäßige, d. h. insbesondere auch gleichmäßige Besteuerung sicherzustellen. Diese im Rechtsstaatsprinzip und im Gleichbehandlungsgebot

[233] *Maunz*, in: ders./Dürig, GG, Art. 108 Rn. 15.

[234] *Schmieszek*, in: Hübschmann/Hepp/Spitaler (Hrsg.), AO/FGO, § 17 FVG Rn. 33; *Krumm*, in: Tipke/Kruse, AO, § 17 FVG Rn. 7.

[235] *Rüsken*, in: Klein, AO, § 30 Rn. 6; *Intemann*, in: Koenig (Hrsg.), AO, § 30 Rn. 5.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

verankerten öffentlichen Interessen haben einen hohen Rang, der über das nur fiskalische Interessen an der Sicherung des Steueraufkommens hinausgeht."[236]

Der Grundsatz digitaler Souveränität im Bereich der Finanzverwaltung ist deshalb nicht nur Ausdruck einer Gewährleistungsverantwortung nach außen, die maßgeblich auf grundrechtlichen Wertungen aufbaut. Wäre dieser nur auf die Grundrechte der einzelnen Steuerpflichtigen zurückzuführen, müsste überlegt werden, ob die Daten der Steuerverwaltung tatsächlich vollumfänglich in dem öffentlich-rechtlichen Einflussbereich verbleiben müssten oder nur in Teilen, sofern dies praktisch realisierbar wäre.[237] Angesichts der Vielfalt der Daten, die im Steuerverfahren herangezogen werden, erschiene es jedenfalls nicht ausgeschlossen, dass im Hinblick auf die Verarbeitung mancher Daten auch private IT-Dienstleister eingebunden werden könnten. Der Grundsatz digitaler Souveränität dient hier aber auch dazu, Vertrauen in das System der Steuererhebung zu schaffen und zu erhalten. Korrespondierend dazu wirken die gesetzlichen Regeln auf die Steuerehrlichkeit der Steuerpflichtigen hin. Der Blick in die Strukturen der Finanzverwaltung macht deutlich, dass einerseits der Grundsatz digitaler Souveränität im konkreten Fall auf verschiedenen Begründungssäulen beruhen kann und andererseits dem Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien eine eigenständige Bedeutung zukommt.

Das Vertrauen prägt daneben maßgeblich Regelungen des Registerwesens, die auf die Herstellung von Publizität abzielen. Publizität steht für die Offenlegung bestimmter Umstände, um entweder Vertrauen im Rechtsverkehr zu begründen oder zu beseitigen.[238] Der Begriff der Publizität steht deshalb in einem engen Zusammenhang mit dem der Öffentlichkeit.[239] Typischerweise findet Publizität im Zivilrecht im Zusammenhang mit öffentlichen Registern Verwendung. Solche Register, wie z. B. das Grundbuch oder Handelsregister, werden mittlerweile elektronisch geführt. Die Frage der Einbindung privater IT-Dienstleister ist auch in diesem Rechtsgebiet nicht einheitlich geregelt.

Nach § 126 Abs. 3 GBO kann die Datenverarbeitung, die für die Führung des Grundbuchs in maschineller Form notwendig ist, im Auftrag des zuständigen Grundbuchamts auf den Anlagen einer anderen staatlichen Stelle oder auf den Anlagen einer juristischen Person des öffentlichen Rechts vorgenommen werden, wenn die ordnungsgemäße Erledigung der Grundbuchsachen sichergestellt ist. Die Führung weiterer Register regelt § 387 Abs. 5 FamFG. Danach kann die elektronische Datenverarbeitung zur Führung des Handels-, Genossenschafts-, Partnerschafts- oder Vereinsregisters im Auftrag des zuständigen Gerichts auf den Anlagen

[236] BVerfGE 67, 100 (139 f.); ebenso BVerfGE 84, 239 (280 f.).

[237] Vgl. oben C. III. 3. b) cc).

[238] Vgl. *Gehrlein*, in: Ebenroth/Boujong/Joost/Strohn, HGB, § 15 Rn. 2; zum Begriff der Publizität auch *Merkt*, Unternehmenspublizität, S. 8 ff.

[239] Vgl. *Marcic*, in: Ehmke/Schmid/Scharoun (Hrsg.), FS Arndt, S. 267 (281); vgl. auch *Smend*, in: Bachof/Drath (Hrsg.), GS W. Jellinek, S. 11 (18).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

einer anderen staatlichen Stelle oder auf den Anlagen eines Dritten vorgenommen werden, wenn die ordnungsgemäße Erledigung der Registersachen sichergestellt ist.

In ihren Voraussetzungen entsprechen sich beide Regelungen und erlauben ein IT-Outsourcing, wenn die ordnungsgemäße Erledigung der Grundbuch- bzw. Registersachen sichergestellt ist. Während aber § 387 Abs. 5 FamFG auch die Einbindung privater IT-Dienstleister ermöglicht, erlaubt § 126 Abs. 3 GBO eine Datenübertragung nur an Stellen, hinter denen Träger staatlicher Gewalt stehen.[240] Diese eingeschränkten Möglichkeiten des § 126 Abs. 3 GBO lassen sich durch die erhebliche Bedeutung dinglicher Rechte an Grundstücken für die wirtschaftliche Position der einzelnen Bürger und Unternehmen erklären.[241] Die verbindliche und öffentlich einsehbare Darstellung der Rechtezuordnung ist ein elementarer Belang für das ordnungsgemäße Funktionieren des Rechtsverkehrs und damit auch für die Bewahrung eines geregelten gesellschaftlichen Miteinanders. Die Teilnehmer des Rechtsverkehrs müssen in einem besonderen Maße auf die Ausführungen des Grundbuchs vertrauen dürfen.[242] Private Unternehmen dürfen in diese Aufgabe nicht eingebunden werden, stattdessen muss das Grundbuch zwingend durch öffentlich-rechtliche Stellen geführt werden.[243] Der Ausschluss privater IT-Dienstleister nach § 126 Abs. 3 GBO ist Ausdruck des Grundsatzes digitaler Souveränität.

Im Gegensatz dazu ermöglicht § 387 Abs. 5 FamFG seinem Wortlaut nach auch eine Einbindung privater IT-Dienstleister, weil die Regelung auch eine Führung der Register auf den Anlagen eines Dritten ermöglicht. Dabei ist aber zu beachten, dass die tatbestandliche Voraussetzung – die ordnungsgemäße Erledigung der Registersachen – als einschränkendes Moment relativ unspezifisch ist. Die Anforderung einer ordnungsgemäßen Erledigung gilt ohnehin für jede staatliche Aufgabenwahrnehmung. Eine Übertragung wäre damit nach § 387 Abs. 5 FamFG möglich, ohne dass private IT-Dienstleister weitergehende Voraussetzungen als öffentliche Stellen vorweisen müssten.

Weitergehende Anforderungen finden sich zum Teil in den Verordnungen zu den einzelnen Registern. Wenn die Datenverarbeitung auf den Anlagen einer anderen staatlichen Stelle oder eines Dritten vorgenommen wird, muss nach § 47 Abs. 2 HRV, § 37 Abs. 1 VRV sichergestellt sein, dass Eintragungen in das Register und der Abruf von Daten hieraus nur erfolgen, wenn dies von dem zuständigen Gericht verfügt worden oder anderweitig zulässig ist.[244] In der Literatur wird bezweifelt, ob im Falle

[240] Vgl. *Wilsch*, in: Hügel (Hrsg.), BeckOK GBO, § 126 Rn. 11; *Demharter*, GBO, § 126 Rn. 15.

[241] BT-Drs. 12/5553, S. 79.

[242] Vgl. *Petri/Dorfner*, ZD 2011, 122 (127).

[243] BT-Drs. 12/5553, S. 79.

[244] Erhöhte Voraussetzungen ergeben sich, wenn die Datenverarbeitung auf Anlagen stattfinden soll, die nicht im Eigentum des Auftragnehmers stehen. In dem Fall muss gewährleistet sein, dass die Daten dem uneingeschränkten Zugriff des Gerichts unterliegen und der Eigentümer der Anlage keinen Zugang zu den Daten hat. Der Ausschluss eines Zugangs zu

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

einer Verlagerung auf Private die notwendige Betriebssicherheit gewährleistet werden kann.[245] Zumindest einer durch Eigenverantwortlichkeit geprägten Übertragung auf Private steht darüber hinaus § 374 FamFG i.V.m. § 23a Abs. 1 Nr. 2, Abs. 2 Nr. 3 GVG entgegen, wonach ausdrücklich das Amtsgericht für die einzelnen Registersachen zuständig ist.[246] Im Falle des Registerwesens sind zwar die spezifischen Gefahren für Daten reduziert, weil die fraglichen Daten ohnehin darauf angelegt sind, durch den Rechtsverkehr wahrgenommen zu werden und die Öffentlichkeit deshalb Kontrollmöglichkeiten hat. Trotzdem entfalten die einzelnen Register i.S.d. § 387 FamFG eine erhebliche Bedeutung für den Rechtsverkehr. Ein Führen der Register durch Träger staatlicher Gewalt und öffentliche IT-Dienstleister wäre deshalb sachgerechter.

V. Zusammenfassung

Der Grundsatz digitaler Souveränität beruht auf dem Institut obligatorischer Staatsaufgaben, einer staatlichen Gewährleistungsverantwortung und dem Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen. Ihm kommt verfassungsrechtlicher Rang zu. Während der Verweis auf obligatorische Staatsaufgaben und deren integrale Bestandteile eine weitergehende Abwägung entbehrlich macht, bedarf es für eine Begründung des Grundsatzes unter Verweis auf eine staatliche Gewährleistungsverantwortung oder das Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien einer Abwägung. Es kann dabei zu Überschneidungen und Ergänzungen kommen. Eine Vielzahl einfachgesetzlicher Vorschriften sind Ausdruck des so verstandenen Grundsatzes digitaler Souveränität, auch wenn dies aus den gesetzlichen Regelungen nicht ausdrücklich hervorgeht. Der Grundsatz digitaler Souveränität unterstützt damit zugleich auch die Herausbildung der notwendigen Fähigkeiten in der Verwaltung, die für einen Einsatz digitaler Informationstechnologien notwendig sind.

---

den Daten dürfte in der Praxis schwer zu realisieren sein. Dabei dürfte es weniger um eine unbefugte Einsicht, Veröffentlichung oder Verwendung der Daten gehen, weil das Register ohnehin auf die Wahrnehmung und Kenntnisnahme durch den Rechtsverkehr angelegt ist. Relevanter dürfte das Verfälschen oder der Verlust von Daten sein.

[245] *Schemmann*, in: Haußleiter (Hrsg.), FamFG, § 387 Rn. 6; *Nedden-Boeger*, in: Schulte-Bunert/Weinreich (Hrsg.), FamFG, § 387 Rn. 17.

[246] *Heinemann*, in: Keidel, FamFG, § 374 Rn. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

D. Vereinbarkeit des Grundsatzes digitaler Souveränität mit unions- und verfassungsrechtlichen Bestimmungen

Der Grundsatz digitaler Souveränität kann dazu führen, dass Träger öffentlicher Gewalt zur Erfüllung bestimmter Aufgaben nicht auf private IT-Dienstleister zurückgreifen dürfen. Als Ausdruck dieses Grundsatzes lassen sich vereinzelt einfachgesetzliche Bestimmungen ausfindig machen, welche die Inanspruchnahme privater IT-Dienstleister ausschließen. Diese Konsequenz muss sich mit unions- und verfassungsrechtlichen Bestimmungen vereinbaren lassen.

I. Vereinbarkeit mit Europäischen Grundfreiheiten und Vergaberecht

Die verfassungsrechtliche Forderung, privatwirtschaftliche Akteure von der Verarbeitung behördlich erhobener Daten zumindest in bestimmten Bereichen auszuschließen, muss insbesondere mit den Grundfreiheiten des europäischen Primärrechts vereinbar sein. Diese garantieren die Niederlassungsfreiheit (Art. 49 AEUV) sowie den freien Waren- und Dienstleistungsverkehr zwischen den Mitgliedsstaaten (Art. 34 f. bzw. Art. 56 AEUV) und werden durch die sekundärrechtlichen Vergaberichtlinien[1] konkretisiert und ergänzt. Insofern stellt sich die Frage, ob ein gesetzliches – gegebenenfalls bereichsspezifisches – Verbot, Aufgaben der Datenverarbeitung auf Privatunternehmen zu übertragen, die unionsrechtlichen Vorgaben verletzen kann.

1. Frühere Rechtsprechung des EuGH

In diese Richtung scheint vor allem ein Urteil des Europäischen Gerichtshofs aus dem Jahr 1989 zu deuten.[2] Damals erklärte das Gericht eine italienische Regelung, welche Privatisierungen im Bereich der Datenvereinbarung einschränkte, für unvereinbar mit der Niederlassungs- und Dienstleistungsfreiheit und der damaligen

[1] Relevant für den Untersuchungsgegenstand sind insoweit die Richtlinie 2014/23/EU des Europäischen Parlaments und des Rates vom 26. 2. 2014 über die Konzessionsvergabe (ABl. EU L 94/1) sowie die Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. 2. 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. EU L 94/65).

[2] EuGH, Urt. v. 5. 12. 1989, Rs. C-3/88, Slg. 1989, 4035.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Vergaberichtlinie. Streitgegenständlich war eine gesetzliche Vorgabe, nach der „Verträge mit dem italienischen Staat über die Einrichtung von Datenverarbeitungssystemen für Rechnung der öffentlichen Verwaltung nur mit Unternehmen geschlossen werden [durften], die unmittelbar oder mittelbar ganz oder mehrheitlich in staatlichem oder öffentlichem Besitz" standen.[3] Der Gerichtshof erblickte in der Regelung eine nicht gerechtfertigte verdeckte Diskriminierung nicht-italienischer Anbieter von Datenverarbeitungssystemen und einen Verstoß gegen vergaberechtliche Ausschreibungspflichten. Das Erfordernis einer mehrheitlichen öffentlichen Beteiligung rechtfertige sich insbesondere nicht aus einem Bedürfnis des Staates, seine Vertragspartner umfassend kontrollieren und ihnen in sicherheitsrelevanten Fragen vertrauen zu können. Denn die angesprochenen Belange könnten gegenüber Unternehmen ohne öffentliche Mehrheitsbeteiligung und deren Mitarbeitern ebenso gut vertraglich gesichert werden.[4]

Diese Einschätzung erscheint angesichts der Besonderheiten datenbezogener Risiken – und insbesondere der faktischen Unumkehrbarkeit von Fehlern – zumindest zweifelhaft, ist für die Zulässigkeit eines *vollständigen* Privatisierungsverbots letztlich aber auch nicht entscheidend. Gegenstand der zitierten Entscheidung war die gesetzliche Vorgabe einer bloß *mehrheitlichen* öffentlichen Beteiligung, die also private Minderheitsbeteiligungen zuließ. Unter diesen Umständen ließ sich ein mittelbarer Eingriff in Grundfreiheiten damit begründen, dass private Beteiligungen an Staatsunternehmen faktisch vor allem von Inländern gehalten werden.[5] Die Probleme resultieren in dieser Konstellation gerade daraus, dass Privaten eine Marktteilnahme – in Form einer Beteiligung an Staatsunternehmen – grundsätzlich ermöglicht wird.[6]

2. Ausschluss Privater als zulässige mitgliedstaatliche Entscheidung

Jede Öffnung eines Beschaffungsmarktes für Private aktiviert zunächst einmal das europäische Vergaberecht. Demgegenüber geht die vorgelagerte Entscheidung darüber, ob eine Gemeinwohlaufgabe überhaupt in den Markt gegeben oder vollständig mit verwaltungseigenen Mitteln erledigt wird („make or buy"), dem uni-

[3] EuGH, Urt. v. 5. 12. 1989, Rs. C-3/88, Slg. 1989, 4035.

[4] EuGH, Urt. v. 5. 12. 1989, Rs. C-3/88, Slg. 1989, 4035, Rn. 10 f.

[5] EuGH, Urt. v. 5. 12. 1989, Rs. C-3/88, Slg. 1989, 4035, Rn. 9.

[6] Ähnlich lag der Fall bei EuGH, Urt. v. 20. 3. 2018, Rs. C-187/16 (Österreichische Stahldruckerei), ECLI:EU:C:2018:194. Hier erklärte das Gericht eine gesetzliche Regelung Österreichs, welche die Herstellung von Pässen ausschließlich der „Österreichische Staatsdruckerei GmbH" vorbehielt, für unvereinbar mit der Niederlassungs- und Dienstleistungsfreiheit sowie den einschlägigen Vergaberichtlinien. Deren einzige Gesellschafterin war die Österreichischen Staatsdruckerei Holding AG, deren Aktien wiederum börsennotiert waren und von Privatpersonen gehalten wurden, a.a.O.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

onsrechtlichen Vergaberecht voraus.[7] Dies entspricht der mittlerweile ständigen Rechtsprechung des Europäischen Gerichtshofs zu den unterschiedlichen Formen der Inhouse-Vergabe.[8] Danach sind jedenfalls solche Beschaffungsvorgänge vergaberechtsfrei, bei denen ein oder mehrere öffentliche Auftraggeber über den Dienstleister (gegebenenfalls gemeinsam) eine Kontrolle wie über eigene Dienststellen ausüben, der Dienstleister im Wesentlichen für den oder die Auftraggeber tätig ist und sämtliche Anteile von der öffentlichen Hand gehalten werden. Eine Direktvergabe von Datenverarbeitungsaufträgen an (gemischt-)öffentliche Unternehmen oder Einrichtungen, die ganz überwiegend für ihre Anteilseigner tätig werden, verstößt daher nicht gegen Vergaberecht. Sogar bloß vertragliche Kooperationen zwischen Kommunen können vom Vergaberecht ausgenommen sein, sofern die Zusammenarbeit der Gebietskörperschaften zur Wahrnehmung einer ihnen allen obliegenden öffentlichen Aufgabe erfolgt.[9] Diese höchstrichterliche Rechtsprechung wurde richtlinienrechtlich aufgegriffen[10] und auf nationaler Ebene in die Regelungen über die öffentlich-öffentliche Zusammenarbeit in § 108 GWB überführt.[11]

Das Europarecht gestattet eine ausschließliche Vergabe von Datenverarbeitungsaufträgen an öffentliche Stellen mithin zumindest „von Fall zu Fall". Eine zuverlässige Absicherung des Grundsatzes digitaler Souveränität streitet indes darüber hinausgehend für gesetzliche Privatisierungsverbote, die dann auch Stellen binden, die möglicherweise gerne ausschreiben würden. Auch insofern stellen die Grundfreiheiten aber kein entscheidendes Hindernis dar, soweit das Privatisierungsverbot umfassend ist, also insbesondere auch gemischt-wirtschaftliche Unternehmen ausschließt. Nationale Handlungsspielräume ergeben sich vor allem aus Art. 345 AEUV, nach welchem die europäischen Verträge die Eigentumsordnungen der Mitgliedsstaaten unberührt lassen. Gemeint ist damit gerade die wirtschaftspolitische Entscheidung der Aufgabenteilung zwischen Staats- und Privatsektor.[12] In seiner Entscheidung in der Rechtssache „Essent" bestätigte der Europäische Gerichtshof, dass Privatisierungsverbote an Art. 345 AEUV zu messen seien und hielt eine niederländische Regelung, die jede private Beteiligung an Energieverteilnetz-

[7] *Gurlit*, in: Burgi/Dreher (Hrsg.), Beck'scher Vergaberechtskommentar I, § 108 GWB Rn. 3.

[8] Siehe etwa EuGH, Urt. v. 18. 11. 1999, Rs. C-107/98 (Teckal), Slg. 1999, I-8121; EuGH, Urt. v. 11. 1. 2005, Rs. C-26/03 (Stadt Halle) Slg. 2005, I-26; für öffentlich-öffentliche Gemeinschaftsunternehmen EuGH, Urt. v. 13. 11. 2008, Rs. C-325/07 (Coditel Brabant), Slg. 2008, I-8486.

[9] EuGH, Urt. v. 9. 6. 2009, Rs. C-480/06 (Stadtreinigung Hamburg), Slg. 2009, I-4762, Rn. 37, 45 ff.

[10] Vgl. Art. 17 RL 2014/23/EU und Art. 12 RL 2014/24/EU.

[11] Zu den verschiedenen von § 108 GWB erfassten Formen der Inhouse-Vergabe näher *Gurlit*, in: Burgi/Dreher (Hrsg.), Beck'scher Vergaberechtskommentar I, § 108 GWB Rn. 8 ff., 20 ff.

[12] *G. Kirchhof*, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, § 15 Rn. 35; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 345 AEUV Rn. 10 ff.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

betreibern untersagte, für unionsrechtlich zulässig.[13] Allgemein führe Art. 345 AEUV zwar nicht zur Unanwendbarkeit der Grundfreiheiten, allerdings stelle das gesetzgeberische Interesse am Ausschluss Privater einen „zwingenden Grund des Allgemeininteresses" dar und könne Beschränkungen der Grundfreiheiten rechtfertigen.[14] Im Hinblick auf die verfolgten Gemeinwohlinteressen dürfte den Mitgliedsstaaten im Lichte von Art. 345 AEUV – auch wenn dieser selbst Eingriffe in Grundfreiheiten noch nicht rechtfertigt[15] – ein beachtlicher Einschätzungsspielraum zuzugestehen sein. Jedenfalls soweit das nationale Verfassungsrecht einer Privatisierung von Datenverarbeitungsaufgaben entgegensteht, wird man zwingende Gemeinwohlgründe kaum verneinen können. Auch ein vollständiger Ausschluss Privater von der Verarbeitung behördlich erhobener Daten wird unionsrechtlich in aller Regel zulässig sein. Neben den besonderen datenspezifischen Risiken[16] lässt sich hierfür insbesondere anführen, dass ein solches Privatisierungsverbot immer noch auf einer Datenerhebung durch die öffentliche Hand aufsetzt und Privaten im Bereich der Datenverarbeitung damit weiterhin eine Vielzahl von Betätigungsmöglichkeiten verbleiben. Wenn aber ein vollständiger Ausschluss Privater vom Betrieb von Energieverteilnetzen unionsrechtlich zulässig ist, spricht einiges für die Zulässigkeit eines solchen bloß teilweisen Ausschlusses Privater von Datenverarbeitungsaufgaben.

Nach alldem stellen die europäischen Grundfreiheiten und die unionsrechtlich geprägten Vorgaben des Vergaberechts den Grundsatz der digitalen Souveränität und seine praktische Umsetzung nicht in Frage.

II. Vereinbarkeit mit der DSGVO

Der Grundsatz digitaler Souveränität wird häufig personenbezogene Daten betreffen, auch wenn dies nicht zwangsläufig der Fall ist. Berührungspunkte können sich deshalb auch mit der DSGVO ergeben, die einen anderen Schutzzweck als die Grundfreiheiten verfolgt.

1. Ausgangssituation

Die Verarbeitung von personenbezogenen Daten durch Dritte wird in der DSGVO durch die Auftragsverarbeitung nach Art. 28 DSGVO geregelt. Wenn es der Grundsatz digitaler Souveränität gebietet, Daten in einer öffentlich-rechtlich geprägten Sphäre zu belassen, ist damit zugleich eine Auftragsverarbeitung unter

[13] EuGH, Urt. v. 22. 10. 2013, Rs. C-105/12 u. a. (Essent), ECLI:EU:C:2013:677.

[14] EuGH, Urt. v. 22. 10. 2013, Rs. C-105/12 u. a. (Essent), ECLI:EU:C:2013:677, Rn. 49 ff.

[15] EuGH, Urt. v. 22. 10. 2013, Rs. C-105/12 u. a. (Essent), ECLI:EU:C:2013:677, Rn. 53.

[16] Dazu oben C. III. 2. b).

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Einbeziehung Privater ausgeschlossen. Die Frage ist, ob dies zu einem Konflikt mit der DSGVO führen kann.

Mit Art. 28, 32 DSGVO werden bestimmte Voraussetzungen formuliert, bei deren Vorliegen eine Auftragsverarbeitung möglich ist. Man könnte sich deshalb auf den Standpunkt stellen, dass mit dem Grundsatz digitaler Souveränität, der nach seiner Konzeption als rechtliches Gebot zu verstehen ist, eine weitere, zusätzliche Voraussetzung formuliert wird, nämlich die der öffentlich-rechtlichen Trägerschaft.

Aus dem Vorhandensein der Regelungen zur Auftragsverarbeitung in der DSGVO lässt sich aber nicht ableiten, dass mögliche private IT-Dienstleister bei der Frage, wer eine konkrete Datenverarbeitung übernimmt, stets berücksichtigt werden müssten. Nur weil private Auftragsverarbeiter auf dem Markt verfügbar sind, bedeutet dies nicht, dass insofern aus den Regelungen zur Auftragsverarbeitung eine Pflicht zu deren Einbindung folgt. Die Art. 28 ff. DSGVO regeln die Zulässigkeit der Auftragsverarbeitung unter datenschutzrechtlichen Gesichtspunkten und befriedigen damit das praktische Bedürfnis nach rechtssicherer Arbeitsteilung.[17] Sie enthalten aber kein Auftragsverarbeitungsgebot. Die Regelungen der DSGVO zur Auftragsverarbeitung betreffen nur das „Wie", nicht aber die Frage, „ob" eine Auftragsverarbeitung durchgeführt wird. Die Entscheidung für Letzteres liegt nach wie vor bei dem Verantwortlichen. Diese Entscheidung und ihre Kriterien sind nicht in den Regelungsbereich der DSGVO einbezogen.

Außerdem zielt der Grundsatz digitaler Souveränität bei genauer Betrachtung auch nicht darauf ab, die Modalitäten der Auftragsverarbeitung zu verändern, sondern knüpft an die öffentlich-rechtliche Rechtsunterworfenheit der Beteiligten an und statuiert Verpflichtungen für diese. Ob dies auch bedeutet, dass das IT-Outsourcing durch eine öffentliche Stelle zugunsten eines öffentlichen IT-Dienstleisters als zulässige Inhouse-Vergabe zugleich mit der DSGVO vereinbar ist, wenn auch private Auftragsverarbeiter zur Verfügung stehen, ist wiederum eine davon zu unterscheidende Frage.

2. Öffnungsklauseln des Art. 6 Abs. 2, 3 DSGVO

Außerdem lässt sich der Grundsatz digitaler Souveränität auch im Rahmen der Öffnungsklauseln des Art. 6 Abs. 2, 3 DSGVO realisieren. Konkret betrifft dies nationale Regelungen wie § 126 Abs. 3 GBO oder §§ 2 Abs. 2, 17 Abs. 3 FVG.[18]

Art. 6 DSGVO enthält die grundlegenden Rechtmäßigkeitsvoraussetzungen für eine Datenverarbeitung. Nach Art. 6 Abs. 1 lit. e DSGVO ist eine Datenverarbeitung unter anderem rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erfor-

[17] *Spoerr*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 28 DSGVO Rn. 1; *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 28 DSGVO Rn. 2.

[18] § 497 StPO fällt wegen Art. 2 Abs. 2 lit. d DSGVO nicht in deren Anwendungsbereich.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

derlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Art. 6 Abs. 3 S. 1 DSGVO bestimmt, dass die Rechtsgrundlagen für Verarbeitungen gemäß Abs. 1 lit. e (und c) entweder durch das Unionsrecht oder das Recht der Mitgliedstaaten festgelegt werden. Und im letztgenannten Fall können die Mitgliedstaaten gemäß Art. 6 Abs. 2 DSGVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 lit. e (und c) beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.

Hinzukommt die Regelung des Art. 6 Abs. 3 DSGVO. Nach dem dortigen S. 3 kann die Rechtsgrundlage des Mitgliedstaats spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung.

Obwohl also die DSGVO einen vollharmonisierenden Ansatz verfolgt,[19] erlauben Art. 6 Abs. 2, 3 DSGVO weitgehende Anpassungen durch die Mitgliedstaaten. Die Verordnung weist in diesem Bereich faktisch den Charakter einer Richtlinie auf.[20]

---

[19] Art. 1 Abs. 3 DSGVO, nachdem darf der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden, lässt sich als Ausdruck eines umfangreichen Harmonisierungsziels der DSGVO verstehen, *Pötters*, in: Gola (Hrsg.), DSGVO, Art. 1 Rn. 24. Auch für die frühere Datenschutzrichtlinie wurde davon ausgegangen, dass ihre Regelungsziele die Unter- und Obergrenze des Datenschutzrechts bilden und eine Vollharmonisierung anstreben, EuGH, Urt. v. 6. 11. 2013, Rs. C-101/01 (Lindqvist), Slg. 2003, I-12971, Rn. 96; vgl. auch EuGH, Urt. v. 16. 12. 2008, Rs. C-524/06 (Huber), Slg. 2008, I-9705, Rn. 51; EuGH, Urt. v. 24. 11. 2011, Rs. C-468/10 und 469/10 (ASNEF), Slg. 2011, I-12181, Rn. 28 f.; EuGH, Urt. v. 19. 10. 2016, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779, Rn. 57 ff.; *Selmayr/Ehmann*, in: dies. (Hrsg.), DS-GVO, 2017, Einführung Rn. 76; *Schantz*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 1 DSGVO Rn. 8; *Pötters*, in: Gola (Hrsg.), DSGVO, Art. 1 Rn. 24. Ein Zurückbleiben hinter den datenschutzrechtlichen Regeln beeinträchtigt grundsätzlich das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 GrCH und weitergehende Bestimmungen behindern den Binnenmarkt und die Grundfreiheiten, *Pötters*, in: Gola (Hrsg.), DSGVO, Art. 1 Rn. 24. Diese Grundsätze werden auch im Rahmen der jetzigen Verordnung, zumal diese im Gegensatz zur Richtlinie unmittelbar gilt, herangezogen, *Selmayr/Ehmann*, in: dies. (Hrsg.), DS-GVO, Einführung Rn. 75 ff.; *Schantz*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 1 DSGVO Rn. 8; *Pötters*, in: Gola (Hrsg.), DSGVO, Art. 1 Rn. 24.

[20] *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 49.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Das Verhältnis von Abs. 2 und Abs. 3 ist eine der bislang nicht geklärten Fragen der DSGVO.[21] Im Folgenden wird auf beide Absätze abgestellt.

a) Anwendungsbereich der Öffnungsklauseln

Die Öffnungsklauseln beziehen sich im Falle des Abs. 1 lit. e auf die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Entscheidend ist hier ein funktionaler Ansatz.[22] Da der Grundsatz digitaler Souveränität von vornherein an die Wahrnehmung staatlicher Aufgaben anknüpft, ist der Anwendungsbereich der Öffnungsklausel insofern eröffnet.

Hinsichtlich der rechtlichen Spezifizierungen und Anpassungen, die dem Mitgliedstaat möglich sind, enthält Art. 6 Abs. 3 S. 3 DSGVO eine Reihe von zulässigen Konkretisierungen. Die dort aufgezählten Modalitäten sind aber nicht abschließend, was schon durch die Formulierung der Verordnung („unter anderem") deutlich wird.[23] Eine nähere Bestimmung zulässiger Auftragsverarbeiter findet sich in der Aufzählung nicht. Genannt werden aber Verarbeitungsvorgänge und Verarbeitungsverfahren, und eine eingrenzende Bestimmung zulässiger Auftragsverarbeiter könnte als Konkretisierung dieser Elemente eingeordnet werden. Diese Überlegung wird durch die Erwägungsgründe der DSGVO gestützt. Demnach kann für mögliche Rechtsgrundlagen nach nationalem Recht festgelegt werden, wer Verantwortlicher im datenschutzrechtlichen Sinne sein soll. Ausdrücklich werden als mögliche Optionen Behörden, juristische Personen des öffentlichen sowie natürliche und juristische Personen des Privatrechts genannt.[24] Wenn durch nationale Anpassungen als Verantwortlicher auch natürliche oder juristische Personen des Privatrechts bestimmt werden können, spricht dies dafür, dass die in Art. 6 Abs. 3 S. 3 DSGVO zugelassenen spezifischen Bestimmungen zur Anpassung der Anwendung der Vorschriften auch Bestimmungen zu Rechtsnatur, Rechtsform oder anzuwendendem Rechtsregime des Auftragsverarbeiters sowie seines Trägers ermöglicht. Die Öffnungsklausel

[21] Vgl. *Albers/Veit*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 59 ff.; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 6 Rn. 93; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 2 DSGVO Rn. 16 ff.

[22] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 DSGVO Rn. 23; *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 51; *Albers/Veit*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 41. Der Annahme einer Aufgabe im öffentlichen Interesse stehen dabei relativ geringe Hürden entgegen, *Reimer*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 6 Rn. 39. Hinsichtlich der Ausübung öffentlicher Gewalt wird die Einordnung der dazugehörigen Aufgabe als öffentliche Aufgabe maßgebliches Gewicht haben, *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 DSGVO Rn. 23, wobei umstritten ist, ob die Regelung von einer Abgrenzung zu hoheitlichen Aufgaben ausgeht, vgl. *Albers/Veit*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 40.

[23] Vgl. *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 6 Rn. 45.

[24] VO (EU) 2016/679, Erwägungsgrund Nr. 45.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

zielt auf weitere Bestimmungen ab, die für die Datenverarbeitung angesichts der spezifisch damit zusammenhängenden Risiken notwendig erscheinen.[25]

Sofern für die Öffnungsklausel des Art. 6 Abs. 2 DSGVO ein eigenständiger Regelungsgehalt angenommen wird, wird dieser weit verstanden; er ermöglicht den Mitgliedstaaten, spezifische Regelungen für ihre inneren Angelegenheiten zu finden.[26] Im Rahmen des Abs. 2 sind den Mitgliedstaaten keine Abweichungen, sondern lediglich Konkretisierungen erlaubt.[27] Diese Befugnis, spezifische Anforderungen präziser zu bestimmen, kann sich auch auf die Person von Auftragsverarbeitern beziehen.[28] Die Eingrenzung des Kreises zulässiger Auftragsverarbeiter, die an die Rechtsform oder das einschlägige Rechtsregime eines Auftragsverarbeiters oder seines Trägers anknüpft, ist als Konkretisierung einzuordnen, wenn zugleich das materielle datenschutzrechtliche Niveau, wie es sich aus Art. 28, 32 DSGVO ergibt, nicht in Frage gestellt wird.

Es ist gerade Sinn und Zweck der Öffnungsklauseln, die Mitgliedstaaten in die Lage zu versetzen, eigenständig gesetzliche Konkretisierungen vorzunehmen, um ihren jeweiligen verfassungsrechtlichen Verpflichtungen nachkommen zu können.[29] Zu diesen zählt auch der Grundsatz digitaler Souveränität. Dies ist auch gerade deshalb notwendig, weil die Regeln der DSGVO zur Auftragsverarbeitung zu pauschal sind und der Vielfalt potenziell erfasster Konstellationen nicht gerecht werden können.[30] Die Regelungen erfassen ebenso die von Privaten durchgeführte Auftragsverarbeitung solcher Daten, die praktisch keine bedeutende Relevanz haben und von den Betroffenen freiwillig weitergegeben wurden, wie auch eine Auftragsverarbeitung höchstsensibler Daten, die Träger staatlicher Gewalt durch die Ausübung hoheitlicher Befugnisse erlangt haben. Die DSGVO erlaubt deshalb gerade in der letzten Konstellation den mitgliedstaatlichen Erlass weitergehender Konkretisierungen.

---

[25] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 3 DSGVO Rn. 47.

[26] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 2 DSGVO Rn. 24 ff.

[27] *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 6 Rn. 29; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 2 DSGVO Rn. 22.

[28] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 2 DSGVO Rn. 27.

[29] *Albers/Veit*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 58; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 6 Rn. 92 ff.; *Spoerr*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 28 DSGVO Rn. 31.1 m.w.N.

[30] In diese Richtung auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, Art. 6 Abs. 2 DSGVO Rn. 1.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

b) Voraussetzungen der Öffnungsklauseln

Die Öffnungsklauseln in Art. 6 Abs. 2, 3 DSGVO verweisen auf unterschiedliche Voraussetzungen. Notwendig ist eine besondere Rechtsgrundlage, die den Zweck der Verarbeitung bestimmt, für die Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, erforderlich und angesichts des Zwecks verhältnismäßig ist.[31] Abs. 2 verlangt außerdem, dass die mitgliedstaatliche Regelung eine rechtmäßige und nach Treu und Glauben erfolgende Datenverarbeitung gewährleistet, wobei dies im Ergebnis regelmäßig keine weitergehenden Anforderungen bewirken dürfte. Im Rahmen des Abs. 2 darf außerdem den Regeln der DSGVO nicht widersprochen und es müssen die spezifischen Umstände und Risiken eines Anwendungsbereichs berücksichtigt werden. Angesichts der Zielrichtung des Grundsatzes digitaler Souveränität lässt sich all dies annehmen.

Für die Qualität der notwendigen Rechtsgrundlage ist die nationale Verfassungsordnung ausschlaggebend, so dass auch untergesetzliche Regelungen dafür in Betracht kommen.[32] Entscheidend ist, dass es sich um eine Rechtsnorm mit unmittelbarer Außenwirkung handelt.[33] Den im Verlaufe dieses Textes dargestellten konkreten Regelungen kann Beispielswirkung zugesprochen werden. Festzuhalten ist aber, dass die Inanspruchnahme der Öffnungsklausel durch den Mitgliedstaat zwingend einer eigenständigen gesetzlichen Regelung bedarf.

Im Falle einer Regelung des zulässigen Kreises an Auftragsverarbeitern braucht regelmäßig keine nähere Zweckbestimmung getroffen zu werden, weil diese schon aus dem zugrundeliegenden Kontext der Datenverarbeitung an sich folgt.[34] Der dort genannte Zweck wird durch die Konkretisierung der Modalitäten der Auftragsverarbeitung nicht in Frage gestellt oder geändert. Bei der Bestimmung zulässiger Auftragsverarbeiter handelt es sich nur um eine Verfahrensregelung. Weiter darf im Ergebnis durch die mitgliedstaatlichen Regeln das Datenschutzniveau der DSGVO nicht unterschritten werden und die Vorgaben der Art. 5, 6 DSGVO müssen eingehalten werden.[35] In diesem Zusammenhang ist vor allem Art. 5 Abs. 1 lit. f DSGVO Beachtung zu schenken. Die Durchsetzung des Grundsatzes digitaler Souveränität dient der Förderung der dort zur grundlegenden Voraussetzung erhobenen Integrität und Vertraulichkeit. Für die Erforderlichkeit der mitgliedstaatlichen Regelung und deren Verhältnismäßigkeit kann auf die Erwägungen zur Begründung des Grundsatzes digitaler Souveränität im konkreten Einzelfall verwiesen werden.

---

[31] *Reimer*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 6 Rn. 39.

[32] *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 6 Rn. 197; *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 198.

[33] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 DSGVO Rn. 35.

[34] Vgl. *Albers/Veit*, in: H. A. Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 57.

[35] *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, Art. 6 Rn. 194; *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 49.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Nach alledem ist festzuhalten: Die DSGVO betrifft schon nicht Regelungen, die darauf abzielen, dass Daten ausschließlich in einer öffentlich-rechtlich geprägten Sphäre verbleiben. Außerdem ließen sich konkrete Bestimmungen auf die Öffnungsklauseln des Art. 6 Abs. 2, 3 DSGVO stützen. Es ist mit der DSGVO vereinbar, wenn die Mitgliedstaaten nationale Regelungen treffen, die den Kreis der zulässigen Auftragsverarbeiter auf öffentliche IT-Unternehmen beschränken. Sollte man dafür die Öffnungsklauseln des Art. 6 Abs. 2, 3 DSGVO heranziehen, bedarf es einer gesetzlichen Regelung.

III. Vereinbarkeit mit Art. 12 Abs. 1 GG

Schließlich wird die Einbindung öffentlicher IT-Dienstleister im Hinblick auf die Berufsfreiheit privater IT-Dienstleister in Zweifel gezogen.[36] Letztendlich kann diese Erwägung aber nicht durchdringen.

Staatliche Konkurrenz bewirkt grundsätzlich keinen Eingriff in die Berufsfreiheit des Art. 12 Abs. 1 GG. Da regelmäßig allenfalls eine mittelbar-faktische Beeinträchtigung in Betracht kommt, bedarf es weitergehender Voraussetzungen.[37] Nach überwiegender Ansicht kann ein Eingriff etwa im Falle schwerer und unerträglicher Wettbewerbsbeeinträchtigungen angenommen werden.[38] Das Eintreten öffentlicher Unternehmen mag zu einer Verschärfung des Wettbewerbs führen, dies dürfte aber die Berufstätigkeit nicht unmöglich machen oder unzumutbar einschränken.

Eine solche Konkurrenzsituation, die zu einem Eingriff führt, kann häufig deshalb schon nicht angenommen werden, weil Träger öffentlicher Gewalt sich von vornherein, gegebenenfalls in Einklang mit § 108 GWB, dazu entscheiden, ausschließlich öffentliche IT-Dienstleister in Anspruch zu nehmen, so dass eine Konkurrenzsituation schon tatsächlich nicht entstehen kann. Sollte sich dies im Einzelfall anders darstellen, wird es in aller Regel an der notwendigen schweren und unerträglichen Wettbewerbsbeeinträchtigung fehlen. Anders mag die Situation möglicherweise bei öffentlichen IT-Dienstleistern sein, deren Betätigungsfeld auch gerade der freie Markt ist, so dass Konkurrenzsituationen zu Privaten tatsächlich entstehen. Wenn diese öffentlichen IT-Dienstleister zugleich in ausschließlichen Vertragsbeziehungen zu Trägern öffentlicher Gewalt stehen, müsste näher untersucht werden, ob solche exklusiven Geschäftsbeziehungen und die dort erwirtschafteten Gewinne derartige Auswirkungen auf die Tätigkeit in anderen Geschäftsfelder haben, dass dadurch ein Eingriff in die Berufsfreiheit privater Konkurrenten anzunehmen ist.

[36] *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 38 ff.

[37] Vgl. auch oben C. I. 2.

[38] BVerwG NJW 1995, 2938 (2939); OVG Münster DÖV 2005, 616 (617); *Burgi*, in: Bonner Kommentar, Art. 12 Abs. 1 Rn. 156; *Kämmerer*, in: von Münch/Kunig, Art. 12 Rn. 50, jeweils m.w.N.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Vereinzelt wird das Modell eines Verwaltungsmonopols[39] herangezogen, um einen Eingriff in die Berufsfreiheit privater Unternehmen zu begründen.[40] Dahinter steht die Annahme, dass Verwaltungsmonopole entstehen, wenn Träger öffentlicher Gewalt bestimmte Aufgaben selbst wahrnehmen oder hierfür ausschließlich öffentliche IT-Dienstleister in Anspruch nehmen. Der damit einhergehende Ausschluss privater IT-Dienstleister sei an der Berufsfreiheit des Art. 12 Abs. 1 GG zu messen.

Nun mag es zutreffen, dass als Folge des Grundsatzes digitaler Souveränität bestimmte, sehr konkret zugeschnittene Tätigkeiten im Einzelfall nicht von Privaten ausgeübt werden können. Bei den ausgeschlossenen Tätigkeiten, etwa der Führung des elektronischen Grundbuchs oder der Speicherung elektronischer Strafakten, wird es sich aber kaum um anerkannte Berufe handeln. Stattdessen wird lediglich das Geschäftsfeld privater IT-Dienstleister beschränkt, nicht aber die Ausübung eines *Berufs* durch ein Verwaltungsmonopol verhindert.

Dies macht deutlich, dass es sich hier allenfalls um das Vorenthalten eines staatlichen Auftrags handeln kann. Im Ausgangspunkt ist insofern festzuhalten, dass ein Anspruch auf Privatisierung gerade nicht besteht.[41] Auch das Vorenthalten eines staatlichen Auftrags kann deshalb grundsätzlich keinen Eingriff in die Berufsfreiheit darstellen.[42] Nur unter bestimmten Umständen kann dies zu einem Eingriff führen. Denkbar wäre etwa eine Beeinträchtigung des Gleichheitssatzes,[43] doch würde dies eine Ungleichbehandlung von Grundrechtsträgern voraussetzen. Im Hinblick auf Art. 12 Abs. 1 GG ist nicht zu erkennen, warum die staatliche Entscheidung, eine Leistung selbst zu erbringen mitsamt ihren faktischen Auswirkungen auf private Unternehmen nicht bloß eine hinzunehmende Gestaltung der Verwaltungsorganisation darstellt, sondern vielmehr eine erhebliche Beeinträchtigung beruflicher Tätigkeiten sein soll.

Wollte man hingegen diesen letztgenannten Standpunkt einnehmen, etwa weil man den Monopolcharakter der konkreten, eng umrissenen Tätigkeit wie der Führung des elektronischen Grundbuchs betont und für maßgeblich hält, wären die Konsequenzen beachtlich: Auch die Entscheidung einer Behörde, die Lagerung und tägliche Verteilung ihrer Akten im Hause durch eigene Behördenmitarbeiter zu erledigen und diese Aufgabe nicht privaten Logistikunternehmen zu überlassen – gewissermaßen die analoge Parallele zum Gegenstand digitaler Souveränität –, müsste einen Eingriff in die Berufsfreiheit bewirken, der durch formelles Gesetz zu rechtfertigen wäre. Und dasselbe müsste streng genommen für eine Vielzahl weiterer Behördentätigkeiten gelten, die nicht Privaten überlassen werden, sondern selbst

[39] Zum Begriff des Verwaltungsmonopols *Badura*, Das Verwaltungsmonopol, S. 86.

[40] *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 40 ff.

[41] Vgl. oben C. I. 2.

[42] *Burgi*, in: Bonner Kommentar, GG, Art. 12 Abs. 1 Rn. 154 f.; *Manssen*, in: v. Mangoldt/Klein/Starck, GG, Art. 12 Rn. 90 ff. Vgl. BVerfGE 116, 135 (161 ff.).

[43] *Manssen*, in: v. Mangoldt/Klein/Starck, GG, Art. 12 Rn. 90.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

erbracht werden. Die weithin anerkannte Absage an eine Privatisierungspflicht würde sich wandeln zu einem gesetzlichen Rechtfertigungszwang für die behördliche Eigenerledigung.

Sollten im Einzelfall ausnahmsweise Umstände vorliegen, die die Annahme eines Eingriffs rechtfertigen, würde es sich regelmäßig lediglich um eine Berufsausübungsregelung handeln. Bei den geschilderten Erwägungen, die den Grundsatz digitaler Souveränität begründen, handelt es sich um vernünftige Gründe des Allgemeinwohls, die eine solche Regelung rechtfertigen würden.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Zusammenfassung in Thesen

1. Für staatliche Daten besteht ein Grundsatz digitaler Souveränität. Dieser kann dazu führen, dass staatliche Daten nicht in private Herrschaftssphären übermittelt werden dürfen, sondern ausschließlich in einem öffentlich-rechtlich geprägten Einflussbereich verbleiben müssen. Dies hat unmittelbare Konsequenzen für IT-Outsourcing durch den Staat und die Möglichkeiten, private oder öffentliche IT-Dienstleister einzubinden.

2. Dem Grundgesetz lassen sich keine ausdrücklichen Vorgaben für diesen Sachbereich entnehmen. Weder existiert ein abgeschlossener Kanon an obligatorischen Staatsaufgaben, noch besteht eine verfassungsrechtliche Pflicht zur Privatisierung. Der Staat ist grundsätzlich nicht verpflichtet, Private in die Wahrnehmung seiner Aufgaben einzubinden, sondern kann diese Aufgaben auch vollständig selbst erbringen.

3. Der Grundsatz digitaler Souveränität hat Verfassungsrang. Er beruht auf dem Institut obligatorischer Staatsaufgaben, einer staatlichen Gewährleistungsverantwortung und dem Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen.

4. In Ausnahmefällen kann es sich bei einer Datenverarbeitung selbst um eine obligatorische Staatsaufgabe handeln. Abseits dessen ist es möglich, dass die Datenverarbeitung integraler Bestandteil einer obligatorischen Staatsaufgabe ist. Dies ist im Wege einer Abwägung festzustellen. Je zentraler ein Datenbestand für die Wahrnehmung einer obligatorischen Staatsaufgabe ist, desto eher dürfen die Daten ausschließlich in einer öffentlich-rechtlich geprägten Sphäre verbleiben. In beiden Fällen ist als Ausdruck des Grundsatzes digitaler Souveränität eine Einbindung privater IT-Dienstleister nicht möglich. Ist die Datenverarbeitung hingegen bloßer Annex zu einer obligatorischen Staatsaufgabe, ist eine Privatisierung – sofern der Grundsatz digitaler Souveränität nicht aus anderen Gründen entgegensteht – möglich.

5. Bei der Einbindung privater IT-Dienstleister in die staatliche Aufgabenwahrnehmung trifft den Staat eine Gewährleistungsverantwortung. Dabei sind besondere Risiken beim Verarbeiten von Daten zu berücksichtigen. Daten als Mittel staatlicher Verwaltungstätigkeit müssen auf der einen Seite verfügbar sein, dürfen nicht inhaltlich oder sonst verfälscht werden, dürfen nicht sachfremd genutzt werden und dürfen nicht unbefugt veröffentlicht werden. Das Risiko einer Realisierung dieser Gefahren steigt, weil Daten einen nicht-rivalen Charakter aufweisen, kostengering und effektiv digital kopiert werden können

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

und eine einmal stattgefundene Wahrnehmung sich realistischerweise nicht mehr rückgängig machen lässt.

6. Für das Verständnis der Gewährleistungsverantwortung verlangt dies nach einem Paradigmenwechsel, weil beim Umgang mit Daten strukturbedingt negative Folgen denkbar sind, die sich unumkehrbar in die Zukunft erstrecken, etwa die unbefugte Veröffentlichung oder ein Datenverlust. Geschehene Fehler lassen sich trotz einer Zurückholung der Aufgabe in die staatliche Sphäre typischerweise nicht mehr rückgängig machen und zeigen dauerhafte Konsequenzen. Eine Privatisierung im Bereich der Datenverarbeitung weist deshalb erhebliche Unterschiede zu anderen, klassischen Privatisierungsfeldern auf. Die allgemeinen Risiken, die generell bei der Einbindung Privater in die Wahrnehmung staatlicher Aufgaben bestehen, wie z. B. Informations- und Machtasymmetrien, fehlende Einflussmöglichkeiten auf den Privaten oder ein Insolvenzrisiko sind im Lichte dieser besonderen Wesensmerkmale von Daten zu berücksichtigen.

7. Die staatliche Gewährleistungsverantwortung richtet sich gleichermaßen nach innen und nach außen. Die nach innen gerichtete Gewährleistungsverantwortung hat die Aufrechterhaltung und Absicherung der Funktionsfähigkeit der Verwaltung zum Ziel. Im Vergleich mit öffentlichen Dienstleistern, etwa als Anstalt des öffentlichen Rechts oder Eigenbetrieb, können private IT-Dienstleister in aller Regel keine vergleichbare finanzielle Versorgung und Stabilität aufweisen und bieten einem staatlichen Auftraggeber keine vergleichbaren rechtlichen Aufsichts- und Einflussmöglichkeiten. Die Fähigkeit zum Verwalten hat für den Staat die Bedeutung einer kritischen Infrastruktur. Die planmäßige Verwendung von Daten ist eine unabdingbare Grundvoraussetzung für die Realisierung der Staatsfunktion Verwaltung. Aufgrund des Grundsatzes digitaler Souveränität kann die Einbindung privater IT-Dienstleister in die staatliche Verwaltungstätigkeit ausgeschlossen sein, weil ansonsten eine faktische Abhängigkeit der Funktionsfähigkeit der staatlichen Verwaltung von Privaten droht. Dies betrifft solche Daten, die für die Funktionsfähigkeit der staatlichen Verwaltung (oder Rechtsprechung bzw. Gesetzgebung) von hoher Bedeutung sind, weil eine Beeinträchtigung ihrer vorgesehenen Nutzung zu erheblichen Defiziten bei der Aufgabenwahrnehmung oder anderen Gefährdungen für die öffentliche Sicherheit führen und sich nicht lediglich als bloße Unbequemlichkeit darstellen würde.

8. Die Gewährleistungsverantwortung nach außen beruht auf dem grundrechtlichen Schutz der Rechtspositionen der Bürgerinnen und Bürger, deren Daten betroffen sind. Die zusätzlichen Einwirkungsmöglichkeiten Privater führen zu einer Gefährdung des Grundrechts auf informationelle Selbstbestimmung und Einschüchterungseffekten, die grundsätzlich nicht durch geringere Kosten oder Effektivitätsgewinne gerechtfertigt werden können. Der Grundsatz digitaler Souveränität kann dazu führen, dass ein hinreichender grundrechtlicher Schutz

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

der Betroffenen nur gewährleistet werden kann, wenn deren Daten ausschließlich in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben. Dabei zu berücksichtigende Faktoren können sein: die Bedeutung der Daten für die Grundrechtswahrnehmung, ihr Bezug zu intimen Sachverhalten, ihre persönlichkeitsbezogene Sensibilität, ihre Attraktivität für Dritte oder die Frage, ob die Datenerhebung mittels hoheitlicher Befugnisse erfolgte.

9. Der Grundsatz digitaler Souveränität basiert daneben auf dem Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen und dabei im Speziellen auf dem Vertrauen in den staatlichen Einsatz digitaler Informationstechnologien. Vertrauen in die Funktionsfähigkeit der Verwaltung ist ein Grundelement der Ausübung von Staatlichkeit und zwingende Voraussetzung für den demokratischen Rechtsstaat. Vertrauen ist entscheidend, wenn Kontrolle fehlt und Unsicherheit herrscht. Durch den Einsatz digitaler Informationstechnologien lösen sich gängige Kontrollstrukturen auf, weil diese an die unmittelbare menschliche Wahrnehmung anknüpfen. Zugleich wecken die Umwälzungen, die mit dem Einsatz digitaler Informationstechnologien (durch den Staat) einhergehen, ein besonderes Bedürfnis nach Vertrauen. Eine Beschädigung des Vertrauens stellt den Einsatz von Informationstechnologien nachhaltig in Frage. Das Maß an Vertrauen, das staatlichen oder privaten Akteuren entgegengebracht wird, ist unterschiedlich groß, weil öffentliche Akteure grundrechtsgebunden sind, dem Vorrang und Vorbehalt des Gesetzes unterworfen sind und ihr Handeln am Gemeinwohl ausgerichtet ist. Aufgrund der Schwierigkeit, Kontrollmechanismen beim Einsatz von Informationstechnologien und beim Umgang mit Daten effektiv zur Geltung zu bringen, sind stattdessen Handlungsgrenzen vorzusehen. Folge des Grundsatzes digitaler Souveränität kann es deshalb sein, gar nicht erst zuzulassen, dass Daten einen öffentlich geprägten Herrschaftsbereich verlassen.

10. Die europäischen Grundfreiheiten und das weitgehend europarechtlich determinierte Vergaberecht stehen der Umsetzbarkeit des Grundsatzes digitaler Souveränität nicht entgegen. Das Vergaberecht ist erst anwendbar, wenn sich die öffentliche Hand zu einer Beschaffung von Datenverarbeitungsdienstleistungen am Markt entschlossen hat und lässt eine ausschreibungsfreie „Inhouse"-Vergabe an öffentliche Stellen und Unternehmen in weitem Umfang zu. Es ist zwar nicht ausgeschlossen, dass gesetzliche Privatisierungsverbote in Grundfreiheiten eingreifen, doch wäre das im hier untersuchten Bereich in aller Regel aus Gründen des Gemeinwohls gerechtfertigt, zumal das Unionsrecht die wirtschaftspolitische Entscheidung über die Aufgabenverteilung zwischen Staats- und Privatsektor in Art. 345 AEUV den Mitgliedstaaten zuweist. Der Grundsatz digitaler Souveränität führt nicht zu einem Konflikt mit den Regeln der Auftragsverarbeitung der DSGVO, weil die DSGVO ebenfalls keine Pflicht zur Auftragsverarbeitung kennt, sondern nur Voraussetzungen für den Fall enthält, dass es tatsächlich zu einer Auftragsverarbeitung kommt. Außerdem bestehen mit Art. 6 Abs. 2, 3 DSGVO Öffnungsklauseln, die es den Mitgliedstaaten er-

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

möglichen, ihren jeweiligen verfassungsrechtlichen Verpflichtungen durch Regelungen des nationalen Rechts Geltung zu verschaffen. Hierzu bedarf es einer gesetzlichen Regelung. Eine Verletzung der Berufsfreiheit privater IT-Dienstleister ergibt sich durch die Umsetzung des Grundsatzes digitaler Souveränität nicht. Der Annahme eines Konkurrenzverhältnisses steht schon der Umstand entgegen, dass öffentliche IT-Dienstleister typischerweise nicht auch am freien Markt tätig sind. Im Übrigen weist ihr Wirken grundsätzlich nicht die notwendige Erheblichkeit auf. Bei der Entscheidung, IT-Dienstleistungen selbst zu erbringen, handelt es sich auch nicht um ein rechtfertigungsbedürftiges Verwaltungsmonopol. Schließlich stellt auch das Vorenthalten staatlicher Aufträge grundsätzlich keinen Eingriff in die Berufsfreiheit dar.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Literaturverzeichnis

Albers, Marion: Grundlagen und Ausgestaltung der Informationsfreiheitsgesetze, in: ZJS 2009, S. 614 – 624.

Auernhammer, Herbert: DSGVO/BDSG, hrsg. von Esser, Martin/Kramer, Philipp/Lewinski, Kai von, 6. Aufl., Köln 2018.

Badura, Peter: Das Verwaltungsmonopol, Berlin 1963.

Baer, Susanne: Vertrauen, Faire Urteile in Wissenschaft und Recht, Göttingen 2013.

Baier, Annette: Vertrauen und seine Grenzen, in: Hartmann, Martin/Offe, Claus (Hrsg.), Vertrauen – Die Grundlage des sozialen Zusammenhalts, Frankfurt/Main 2001, S. 37 – 84.

Battis, Ulrich (Hrsg.): Bundesbeamtengesetz, 5. Aufl., München 2017.

Becker, Florian/*Blackstein*, Ylva: Der transparente Staat – Staatliche Verbraucherinformation über das Internet, in: NJW 2011, S. 490 – 494.

Becker, Siegfried/*Oldenhage*, Klaus: Bundesarchivgesetz, München 2007.

Benda, Ernst: Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, in: DuD 1984, S. 86 – 90.

Berger, Ariane: Digitales Vertrauen – Eine verfassungs- und verwaltungsrechtliche Perspektive, in: DVBl. 2017, S. 804 – 808.

Böckenförde, Ernst-Wolfgang: Die Methoden der Verfassungsinterpretation – Bestandsaufnahme und Kritik, in: NJW 1976, S. 2089 – 2099.

Boehme-Neßler, Volker: Vertrauen im Internet – Die Rolle des Rechts, in: MMR 2009, S. 439 – 444.

Bonner Kommentar zum Grundgesetz, hrsg. von Kahl, Wolfgang/Waldhoff, Christian/Walter, Christian, 199. Ergänzungslieferung, Heidelberg 2019.

Braun Binder, Nadja: Vollständig automatisierter Erlass eines Verwaltungsaktes und Bekanntgabe über Behördenportale, in: DÖV 2016, S. 891 – 898.

Bull, Hans-Peter: Der „vollständig automatisiert erlassene" Verwaltungsakt – Zur Begriffsbildung und rechtlichen Einhegung von „E-Government", in: DVBl. 2017, S. 409 – 417.

Bull, Hans-Peter: Die Staatsaufgaben nach dem Grundgesetz, Kronberg/Ts. 1977.

Burgi, Martin: Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 67. DJT, Bd. 1, München 2008, Gutachten D.

Burgi, Martin: Privatisierung, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Bd. IV, Aufgaben des Staates, 3. Aufl., Heidelberg 2006, § 75, S. 205 – 242.

Burgi, Martin: Vergabefremde Zwecke und Verfassungsrecht, in: NZBau 2001, S. 64 – 72.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Burgi, Martin/*Dreher*, Meinrad (Hrsg.): Beckscher Vergaberechtskommentar, Bd. 1, Gesetz gegen Wettbewerbsbeschränkungen – GWB – 4. Teil, 3. Aufl., München 2017.

Calliess, Christian/*Ruffert*, Matthias (Hrsg.): EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 5. Aufl., München 2016.

Conrad, Isabell/*Strittmatter*, Marc: Cloud Computing, in: Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch zum IT- und Datenschutzrecht, 2. Aufl., München 2016.

Debski, Andrzej: Cloud-Risiken und wie Anwenderunternehmen ihnen begegnen sollten, Wo liegen die typischen Probleme und welche Maßnahmen sind State-of-the-Art?, in: DuD 2016, S. 659 – 666.

Demharter, Johann: Grundbuchordnung, 31. Aufl., München 2018.

Diering, Björn/*Timme*, Hinnerk (Hrsg.): SGB X – Sozialverwaltungsverfahren und Sozialdatenschutz, Lehr- und Praxiskommentar, 5. Aufl., Baden-Baden 2019.

Dörr, Dieter: Informationsfreiheit, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. IV, Grundrechte in Deutschland – Einzelgrundrechte I, Heidelberg 2011, § 103, S. 965 – 1018.

Dreher, Meinrad: Die Kontrolle des Wettbewerbs in Innovationsmärkten, Marktabgrenzung und Marktbeherrschung in innovationsgeprägten Märkten, in: ZWeR 2009, S. 149 – 175.

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, Bd. I, Präambel, Art. 1 – 19, 3. Aufl., Tübingen 2013.

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, Bd. II, Art. 20 – 82, 3. Aufl., Tübingen 2015.

Druey, Jean Nicolas: Information als Gegenstand des Rechts, Entwurf einer Grundlegung, Zürich 1995.

Ebenroth, Carsten Thomas/*Boujong*, Karlheinz/*Joost*, Detlev/*Strohn*, Lutz, Handelsgesetzbuch, Bd. 1, §§ 1 – 342e, hrsg. von Joost, Detlev/Strohn, Lutz, 3. Aufl., München 2014.

Egloff, Willi: Information und Grundrechte, in: DVR 7 (1978), S. 115 – 150.

Ehmann, Eugen/*Selmayr*, Martin (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., München 2018.

Eichenhofer, Johannes: Privatheit im Internet als Vertrauensschutz, Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, in: Der Staat 55 (2016), S. 41 – 67.

Emmert, Ulrich: Europäische und nationale Regulierungen, Konsequenzen für den Datenschutz nach dem Ende von Safe Harbor, in: DuD 2016, S. 34 – 37.

Ernst, Christian: Die Wahrnehmung des öffentlichen Hausrechts durch private Sicherheitsdienste, in: NVwZ 2015, S. 333 – 338.

Faber, Eberhard von: Organisation und Absicherung einer industriellen IT-Produktion, Drei Handlungsfelder jenseits von „Protection, Detection, Reaction", in: DuD 2016, S. 647 – 653.

Fichert, Frank/*Sohns*, Anne: Wettbewerbsschutz auf dem Markt für Server-Betriebssysteme, Wettbewerbspolitische Anmerkungen zur Microsoft-Entscheidung der EU-Kommission, in: WuW 2004, S. 907 – 917.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Fischer, Kristian/*Fluck*, Jürgen: Informationsfreiheit versus Betriebs- und Geschäftsgeheimnisse, in: NVwZ 2013, S. 337 – 340.

Fleischer, Holger/*Körber*, Torsten: Marktmacht, Machtmissbrauch und Microsoft, Zur Rolle des Kartellrechts in der New Economy, in: K&R 2001, S. 623 – 631.

Fox, Dirk: Vertrauen, in: DuD 2015, S. 328 – 328.

Franzius, Claudio: Der „Gewährleistungsstaat" – Ein neues Leitbild für den sich wandelnden Staat?, in: Der Staat 42 (2003), S. 493 – 517.

Frevert, Ute: Vertrauen – eine historische Spurensuche, in: dies. (Hrsg.), Vertrauen – Historische Annäherungen, Göttingen 2003, S. 7 – 66.

Gaycken, Sandro: Informationelle Selbstbestimmung und narrativistische Rezeption, Zur Konstruktion informationellen Vertrauens, in: DuD 2011, S. 346 – 350.

Gern, Alfons/*Brüning*, Christoph: Deutsches Kommunalrecht, 4. Aufl., Baden-Baden 2019.

Gey, Peter: Das Berufungsurteil in Sachen Microsoft – Kartellrecht in dynamischen Technologiemärkten, in: WuW 2001, S. 933 – 944.

Gitter, Rotraud/*Meißner*, Alexander/*Spauschus*, Philipp: Das IT-Sicherheitsgesetz, Sicherheit und Datenschutz – gemeinsames Ziel oder Widerspruch?, in: DuD 2016, S. 7 – 11.

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., München 2018.

Graf, Jürgen-Peter (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 33. Edition, München 2018.

Griesser, Marcus/*Buntschu*, Werner: Vertrauen oder Wissen? Eine Risikobetrachtung für sicheres IT-Outsourcing, in: DuD 2016, S. 640 – 646.

Grimm, Rüdiger/*Maier*, Michaela/*Rothmund*, Tobias: Vertrauen, Ein interdisziplinäres Referenzmodell, in: DuD 2015, S. 283 – 288.

Grobauer, Bernd/*Kossakowski*, Klaus-Peter/*Schreck*, Thomas: Klassifikation von IT-Sicherheitsvorfällen, in: DuD 2016, S. 17 – 21.

Grudzien, Waldemar: IT-Sicherheitsgesetz – Gedanken zur Implementierung, in: DuD 2016, S. 29 – 33.

Gründer, Torsten: Partnerschaftsgestaltung für sicheres IT-Outsourcing, Das schwierige Verhältnis von Anwendern und Dienstleistern, wichtigste Handlungsfelder im Rahmen des OMIT-Referenzmodells, in: DuD 2016, S. 667 – 674.

Grundmann, Cornelia/*Greve*, Holger: Löschung und Vernichtung von Akten, Ordnungsgemäße Aktenführung im Spannungsfeld zum Datenschutz, in: NVwZ 2015, S. 1726 – 1730.

Haußleiter, Martin (Hrsg.): FamFG, Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit, 2. Aufl., München 2017.

Heckmann, Dirk: jurisPK-Internetrecht, 6. Aufl., Saarbrücken 2019.

Heckmann, Dirk: Vertrauen in virtuellen Räumen?, Rechtssichere Internetnutzung zwischen Fake und Faszinosum, in: K&R 2010, S. 1 – 7.

Heckmann, Dirk: IT-Outsourcing der Öffentlichen Hand, in: Bräutigam, Peter (Hrsg.), IT-Outsourcing und Cloud Computing, 4. Aufl., Berlin 2019, Teil 10.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Heckmann, Dirk/*Bernhardt*, Wilfried: Digitale Gewaltenteilung als Marktverantwortung, Kriterien zur rechtlichen Abgrenzung staatlicher und privatwirtschaftlicher Entfaltungsmöglichkeiten auf dem Markt der IT-Herstellung und IT-Services, Eine Studie im Auftrag des Verbandes der mittelständischen IT-Dienstleister und Softwarehersteller für den öffentlichen Sektor, DATABUND e.V., Passau/Berlin 2016.

Heckmann, Dirk/*Braun*, Frank: Datenverarbeitung durch private IT-Dienstleister im Meldewesen, in: BayVBl. 2009, S. 581 – 586.

Heintschel-Heinegg, Bernd von (Hrsg.): Beck'scher Online-Kommentar StGB, 42. Edition, München 2019.

Heintzen, Markus: Behördliches Informationshandeln bei ungewissem Sachverhalt, Zugleich zur Frage der Übertragbarkeit zivilrechtlicher Grundsätze auf behördliches Informationshandeln, in: NuR 1991, S. 301 – 306.

Helm, Thorsten Matthias: Rechtspflicht zur Privatisierung, Baden-Baden 1999.

Hengstschläger, Johannes: Privatisierung von Verwaltungsaufgaben, in: VVDStRL 54 (1995), S. 165 – 203.

Hoffmann-Riem, Wolfgang: Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, in: AöR 134 (2009), S. 513 – 541.

Hoffmann-Riem, Wolfgang: Verantwortungsteilung als Schlüsselbegriff moderner Staatlichkeit, in: Kirchhof, Paul/Lehner, Moris/Raupach, Arndt/Rodi, Michael (Hrsg.), Staaten und Steuern, Festschrift für Klaus Vogel zum 70. Geburtstag, Heidelberg 2000, S. 47 – 64.

Hornung, Gerrit: Ein neues Grundrecht – Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, in: CR 2008, S. 299 – 306.

Hornung, Gerrit: Zwei runde Geburtstage – Das Recht auf informationelle Selbstbestimmung und das WWW, in: MMR 2004, S. 3 – 8.

Huber, Hans: Vertrauen und Vertrauensschutz im Rechtsstaat, in: Häfelin, Ulrich/Haller, Walter/Schindler, Dietrich (Hrsg.), Menschenrechte – Föderalismus – Demokratie, Festschrift zum 70. Geburtstag von Werner Kägi, Zürich 1979, S. 193 – 208.

Hübschmann, Walter/*Hepp*, Ernst/*Spitaler*, Armin (Hrsg.): Abgabenordnung – Finanzgerichtsordnung, 252. Lfg., Köln 2019.

Hügel, Stefan (Hrsg.): Beck'scher Onlinekommentar GBO, 36. Edition, München 2019.

Isensee, Josef: Staatsaufgaben, in: ders./Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Bd. IV, Aufgaben des Staates, 3. Aufl., Heidelberg 2006, § 73, S. 117 – 160.

Jarass, Hans D./*Pieroth*, Bodo: Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 15. Aufl., München 2018.

Jarass, Hans D.: Funktionen und Dimensionen der Grundrechte, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Bd. II, Grundrechte in Deutschland – Allgemeine Lehren I, Heidelberg 2006, § 38, S. 625 – 654.

Kaiser, Anna-Bettina: Die Kommunikation der Verwaltung, Diskurse zu den Kommunikationsbeziehungen zwischen staatlicher Verwaltung und Privaten in der Verwaltungsrechtswissenschaft der Bundesrepublik Deutschland, Baden-Baden 2009.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Kämmerer, Jörn Axel: Privatisierung, Typologie – Determinanten – Rechtspraxis – Folgen, Tübingen 2001.

Käß, Robert: Die Warnung als verwaltungsrechtliche Handlungsform, in: WiVerw 2002, S. 197 – 211.

Keidel, Theodor: FamFG, Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit, Kommentar, hrsg. von Engelhardt, Helmut/Sternal, Werner, 19. Aufl., München 2017.

Kemmler, Iris: Die Anstaltslast, Berlin 2001.

Kirchhof, Gregor: Europäische Integration und Privatisierungen, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 15, S. 585 – 618.

Kirchhof, Paul: Recht lässt hoffen, München 2014.

Klein, Franz: Abgabenordnung – einschließlich Steuerstrafrecht, Kommentar, 14. Aufl., München 2018.

Knauff, Matthias: Die wirtschaftliche Betätigung der öffentlichen Hand, in: Schmidt, Reiner/Wollenschläger, Ferdinand (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 4. Aufl., Heidelberg 2016.

Knemeyer, Franz-Ludwig: Privatisierung und modernes kommunales Unternehmensrecht, Eigengesellschaft oder Kommunalunternehmen in der Rechtsform der Anstalt des öffentlichen Rechts als Gegenbewegung zur Privatisierung, in: Juridica International 2009, S. 22 – 32.

Koenig, Ulrich (Hrsg.): Abgabenordnung: 3. Aufl., München 2014.

Könen, Andreas: IT-Sicherheit gesetzlich geregelt, Kooperationen gestalten, Umsetzung steuern, in: DuD 2016, S. 12 – 16.

Krause, Peter: Rechtsformen des Verwaltungshandelns, Überlegungen zu einem System der Handlungsformen der Verwaltung, mit Ausnahme der Rechtsetzung, Berlin 1974.

Kubicek, Herbert: Vertrauen durch Sicherheit – Vertrauen in Sicherheit, Annäherung an ein schwieriges Verhaltnis, in: Klumpp, Dieter/Kubicek, Herbert/Roßnagel, Alexander/Schulz, Wolfgang (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, Berlin 2008, S. 17 – 36.

Kuhlen, Rainer: Vertrauen in elektronischen Raumen, in: Klumpp, Dieter/Kubicek, Herbert/Roßnagel, Alexander/Schulz, Wolfgang (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, Berlin 2008, S. 37 – 52.

Kühling, Jürgen/*Buchner*, Benedikt (Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Landesrechnungshof Mecklenburg-Vorpommern, Jahresbericht 2019, Teil 1 Landesfinanzbericht 2019, abrufbar unter https://www.lrh-mv.de/static/LRH/Dateien/Jahresberichte/LFB_2019.pdf, zuletzt abgerufen am 16. 8. 2019.

Locke, John: Zwei Abhandlungen über die Regierung, Frankfurt/Main 1977.

Luhmann, Niklas: Vertrauen, Ein Mechanismus der Reduktion sozialer Komplexität, 5. Aufl., Konstanz 2014.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Mangoldt, Hermann von/*Klein*, Friedrich/*Starck*, Christian: Grundgesetz, Kommentar, hrsg. von Huber, Peter M./Voßkuhle, Andreas, 7. Aufl., München 2018.

Marcic, René: Die Öffentlichkeit als Prinzip der Demokratie, in: Ehmke, Horst/Schmid, Carol/Scharoun, Hans (Hrsg.), Festschrift für Adolf Arndt zum 65. Geburtstag, Frankfurt/Main 1969, S. 267 – 292.

Marenbach, Ulrich: Die informationellen Beziehungen zwischen Meldebehörde und Polizei in Berlin, Historische, verfassungsrechtliche und dogmatische Aspekte der Zusammenarbeit, Berlin 1995.

Martini, Mario unter Mitarbeit von Fritzsche, Saskia und Kolain, Michael: Digitalisierung als Herausforderung und Chance für Staat und Verwaltung, Speyer 2016.

Maunz, Theodor/*Dürig*, Günter: Grundgesetz, Kommentar, hrsg. von Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H., 86. Lfg, München 2019.

Maurer, Hartmut: Kontinuitätsgewähr und Vertrauensschutz, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Bd. IV, Aufgaben des Staates, 3. Aufl., Heidelberg 2006, § 73, S. 117 – 160.

Mayer-Schönberger, Viktor: Information als Gestaltungsaufgabe – Eine transatlantische Begegnung, in: Schweizer, Rainer J./Burkert, Herbert/Gasser, Urs (Hrsg.), Festschrift für Jean Nicolas Druey zum 65. Geburtstag, Zürich 2002, S. 853 – 868.

Mayer-Schönberger, Viktor: Informationsrecht für die Informationsgesellschaft, in: SJZ 97 (2001), S. 383 – 388.

Merkt, Hanno: Unternehmenspublizität, Die Offenlegung von Unternehmensdaten als Korrelat der Marktteilnahme, Tübingen 2001.

Meyer-Ladewig, Jens/*Nettesheim*, Martin/*von Raumer*, Stefan (Hrsg.): EMRK, Handkommentar, 4. Aufl., Baden-Baden 2017.

Möllering, Guido: Grundlagen des Vertrauens, Wissenschaftliche Fundierung eines Alltagsproblems, in: Max-Planck-Institut für Gesellschaftsforschung (Hrsg.), Jahrbuch 2007 – 2008, S. 73 – 78.

Münch, Ingo von/*Kunig*, Philip (Hrsg.): Grundgesetz, Band 1, 6. Aufl., München 2012.

Musielak, Hans-Joachim/*Voit*, Wolfgang (Hrsg.): Zivilprozessordnung mit Gerichtsverfassungsgesetz, Kommentar, 16. Aufl., München 2019.

Ossenbühl, Fritz: Verbraucherschutz durch Information, in: NVwZ 2011, S. 1357 – 1363.

Ossenbühl, Fritz: Vertrauensschutz im sozialen Rechtsstaat, in: DÖV 1972, S. 25 – 36.

Oswald, Margit E.: Vertrauen – eine Analyse aus psychologischer Sicht, in: Hof, Hagen/Kummer, Hans/Weingart, Peter/Maasen, Sabine (Hrsg.), Recht und Verhalten, Verhaltensgrundlagen des Rechts – zum Beispiel Vertrauen, Baden-Baden 1994, S. 111 – 128.

Ott, Sascha: Information, Zur Genese und Anwendung eines Begriffs, Konstanz 2004.

Paal, Boris P./*Pauly*, Daniel A. (Hrsg.): Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Peters, Hans: Öffentliche und staatliche Aufgaben, in: Dietz, Rolf/Hübner, Heinz (Hrsg.), Festschrift für Hans Carl Nipperdey zum 70. Geburtstag, Bd. II, München und Berlin 1965, S. 877 – 895.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Petri, Thomas/*Dorfner*, Claudia: E-Justiz und Datenschutz – Ausgewählte Rechtsfragen, in: ZD 2011, S. 122 – 128.

Picot, Arnold: Mehrwert von Information – betriebswirtschaftliche Perspektiven, in: Kubicek, Herbert/Klumpp, Dieter/Müller, Günter/Neu, Werner/Raubold, Eckart/Roßnagel, Alexander (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1997, Die Ware Information – Auf dem Weg zu einer Informationsökonomie, Heidelberg 1997, S. 42 – 59.

Pohlmann, Norbert: Zur Entwicklung einer IT-Sicherheitskultur, Wie das IT-Sicherheitsgesetz den gesellschaftlichen Umgang mit IT-Risiken fördern kann, in: DuD 2016, S. 38 – 42.

Poscher, Ralf: Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander, Hans-Helmut/Perron, Walter/Poscher, Ralf u. a. (Hrsg.), Resilienz in der offenen Gesellschaft, Baden-Baden 2012, S. 167 – 190.

Püschel, Jan Ole: Informationen des Staates als Wirtschaftsgut, Berlin 2006.

Rammos, Thanos/*Vonhoff*, Hans: Cloud Computing und Sozialdatenschutz, Rechtliche Rahmenbedingungen für den Einsatz von Cloud Computing-Diensten im Sozialleistungssektor, in: CR 2013, S. 265 – 272.

Reinhardt, Markus: Wissen und Wissenszurechnung im öffentlichen Recht, Unter besonderer Berücksichtigung von Anforderungen an die Organisation und Folgen ihrer Verletzung im Rahmen öffentlich-rechtlicher Verwaltungstätigkeit, Berlin 2010.

Röhl, Hans Christian: Verwaltungsverantwortung als dogmatischer Begriff?, in: Die Verwaltung Beiheft 2, Die Wissenschaft vom Verwaltungsrecht, Werkstattgespräch aus Anlaß des 60. Geburtstags von Prof. Dr. Eberhard Schmidt-Aßmann, Berlin 1999, S. 33 – 56.

Roßnagel, Alexander/*Richter*, Philipp/*Nebel*, Maxi: Internet Privacy aus rechtswissenschaftlicher Sicht, in: Buchmann, Johannes (Hrsg.), Internet Privacy, Eine multidisziplinäre Bestandsaufnahme, Berlin 2012, S. 281 – 326.

Ruschemeier, Hannah: Der additive Grundrechtseingriff, Berlin 2019.

Sachs, Michael (Hrsg.): Grundgesetz, Kommentar, 8. Aufl., München 2018.

Satzger, Helmut/Schluckebier, Wilhelm/Widmaier, Gunter (Hrsg.), Strafprozessordnung mit GVG und EMRK, Kommentar, 3. Aufl., Köln 2018.

Schaal, Gary S.: Vertrauen, Verfassung und Demokratie, Über den Einfluss konstitutioneller Prozesse und Prozeduren auf die Genese von Vertrauensbeziehungen in modernen Demokratien, Wiesbaden 2004.

Schmelling, Heinz-Dieter: Motivation – Wie verhält sich die IT-Sicherheit zum IT-Outsourcing?, Eine Bestandsaufnahme, in: DuD 2016, S. 635 – 639.

Schoch, Friedrich: Amtliche Publikumsinformation zwischen staatlichen Schutzauftrag und Staatshaftung, Das Verbraucherinformationsrecht als Modell der amtlichen Publikumsinformation, in: NJW 2012, S. 2844 – 2850.

Schoch, Friedrich: Entformalisierung staatlichen Handelns, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Bd. III, Demokratie – Bundesorgane, 3. Aufl., Heidelberg 2005, § 37, S. 131 – 228.

Schoch, Friedrich: Informationsfreiheitsgesetz, Kommentar, 2. Aufl., München 2016.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Schoch, Friedrich: Neuere Entwicklungen im Verbraucherinformationsrecht, in: NJW 2010, S. 2241 – 2247.

Schoch, Friedrich: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 158 – 212.

Schönke, Adolf/*Schröder*, Horst: Strafgesetzbuch, Kommentar, 30. Aufl., München 2019.

Schrotz, Jan-Oliver/*Zdanowiecki*, Konrad: Cloud Computing für die öffentliche Hand, Rechtliche Schlüsselthemen und Lösungsansätze, in: CR 2015, S. 485 – 492.

Schubert, Annegret: Privatisierung des eGovernment, Stuttgart 2009.

Schulte-Bunert, Kai/*Weinreich*, Gerd (Hrsg.): FamFG, Kommentar, 5. Aufl., Köln 2016.

Schulz, Gabriel: Informationssicherheit in Kommunen, Voraussetzung für den Datenschutz der Bürgerinnen und Bürger, in: DuD 2015, S. 466 – 471.

Schulze-Fielitz, Helmuth: Grundmodi der Aufgabenwahrnehmung, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.): Grundlagen des Verwaltungsrechts, Bd. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München 2012, § 12, S. 823 – 902.

Schuppert, Gunnar Folke (Hrsg.): Der Gewährleistungsstaat – Ein Leitbild auf dem Prüfstand, Baden-Baden 2005.

Schuppert, Gunnar Folke: Der Gewährleistungsstaat – modisches Label oder Leitbild sich wandelnder Staatlichkeit?, in: ders. (Hrsg.), Der Gewährleistungsstaat – Ein Leitbild auf dem Prüfstand, Baden-Baden 2005, S. 11 – 52.

Schuppert, Gunnar Folke: Staatswissenschaft, Baden-Baden 2003.

Schwartmann, Rolf/*Jaspers*, Andreas/*Thüsing*, Gregor/*Kugelmann*, Dieter (Hrsg.): DS-GVO/BDSG, Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz, Heidelberg 2018.

Schwarz, Kyrill-Alexander: Vertrauensschutz als Verfassungsprinzip, Eine Analyse des nationalen Rechts, des Gemeinschaftsrechts und der Beziehungen zwischen beiden Rechtskreisen, Baden-Baden 2002.

Siegel, Thorsten: Automatisierung des Verwaltungsverfahrens – zugleich eine Anmerkung zu §§ 35a, 24 I 3, 41 IIa VwVfG, in: DVBl. 2017, S. 24 – 28.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014.

Simitis, Spiros/*Hornung*, Gerrit/*Spiecker gen. Döhmann* (Hrsg.): Datenschutzrecht, 9. Aufl., Baden-Baden 2019.

Simmel, Georg: Soziologie, Untersuchungen über die Formen der Vergesellschaftung, Gesamtausgabe, Bd. 11, Soziologie, 8. Aufl., Frankfurt/Main 2016.

Smend, Rudolf: Zum Problem des Öffentlichen und der Öffentlichkeit, in: Bachof, Otto/Drath, Martin (Hrsg.), Forschungen und Berichte aus dem öffentlichen Recht, Gedächtnisschrift für Walter Jellinek, München 1955, S. 11 – 20.

Spinner, Helmut F.: Ist Wissen analogiefähig?, Über Sach-, Geld-, Wasser- und andere Vergleiche, in: Schweizer, Rainer J./Burkert, Herbert/Gasser, Urs (Hrsg.), Festschrift für Jean Nicolas Druey zum 65. Geburtstag, Zürich 2002, S. 947 – 970.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Stegmüller, Martin: Vollautomatische Verwaltungsakte – eine kritische Sicht auf die neuen § 24 I 3 und § 35 a VwVfG, in: NVwZ 2018, S. 353 – 358.

Steinmüller, Wilhelm u. a.: Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Inneren, in: BT-Drs. 6/3826, S. 5 – 211.

Stelkens, Paul/*Bonk*, Heinz Joachim/*Sachs*, Michael (Hrsg.): Verwaltungsverfahrensgesetz, Kommentar, 9. Aufl., München 2018.

Stopper, Martin: Der Microsoft-Beschluss des EuG, Anwendung des kartellrechtlichen Missbrauchsverbots auf ein durch gewonnenen Innovationswettbewerb entstandenes natürliches Monopol innerhalb eines dynamischen Marktes, in: ZWeR 2005, S. 87 – 110.

Stransfeld, Reinhard: Rechtliche Herausforderungen der Informationsgesellschaft, in: Tauss, Jörg/Kollbeck, Johannes/Mönikes, Jan (Hrsg.), Deutschlands Weg in die Informationsgesellschaft, Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 684 – 708.

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl., Baden-Baden 2018.

Thiele, Alexander: Art. 33 Abs. 4 GG als Privatisierungsschranke, Zugleich Anmerkung zum Urteil des Niedersächsischen Staatsgerichtshofs vom 05.12. 2008, 2/07, in: Der Staat 49 (2010), S. 274 – 298.

Tinnefeld, Marie-Theres: Freiheit in der digitalen Gesellschaft? Zu den Bedingungen von Selbstbestimmung und Kommunikation, in: RDV 2009, S. 47 – 51.

Tipke, Klaus/*Kruse*, Heinz Wilhelm: Abgabenordnung – Finanzgerichtsordnung, Kommentar, 156. Lfg., Köln 2019.

Ulmer, Claus D.: IT-Outsourcing und Datenschutz bei der Erfüllung öffentlicher Aufgaben, in: CR 2003, S. 701 – 707.

Vassilaki, Irini E.: Das Prinzip Vertrauen für Informationsdienste, Über die Entwicklung rechtlicher Rahmenbedingungen innerhalb der Informationsdienstebeziehungen, in: CR 2002, S. 742 – 747.

Vesting, Thomas: Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.): Grundlagen des Verwaltungsrechts, Bd. II, Informationsordnung, Verwaltungsverfahren, Handlungsformen, 2. Aufl., München 2012, § 20, S. 1 – 34.

Vogelsang, Klaus/*Lübking*, Uwe/*Ulbrich*, Ina-Maria: Kommunale Selbstverwaltung, 3. Aufl., Berlin 2005.

Voßkuhle, Andreas: Beteiligung Privater an öffentlichen Aufgaben und staatliche Verantwortung, in: VVDStRL 62 (2003), S. 266 – 335.

Voßkuhle, Andreas: Gesetzgeberische Regelungsstrategien der Verantwortungsteilung zwischen öffentlichem und privatem Sektor, in: Schuppert, Gunnar Folke (Hrsg.), Jenseits von Privatisierung und „schlankem" Staat, Verantwortungsteilung als Schlüsselbegriff eines sich verändernden Verhältnisses von öffentlichem und privatem Sektor, Baden-Baden 1999, S. 47 – 90.

Weichert, Thilo: Vertrauen in die Vertraulichkeit bei der elektronischen Gesundheitskarte, in: GesR 2005, S. 151 – 155.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Weilert, Katarina: Das paradoxe Vertrauen gegenüber dem Staat und seinen Institutionen, in: HFR 2010, S. 207 – 229.

Weiß, Wolfgang: Privatisierung und Staatsaufgaben, Privatisierungsentscheidungen im Lichte einer grundrechtlichen Staatsaufgabenlehre unter dem Grundgesetz, Tübingen 2002.

Werres, Stefan: Das Outsourcing der Beihilfebearbeitung aus verfassungsrechtlicher Sicht, in: ZBR 2001, S. 429 – 436.

Wissenschaftlicher Dienst des Bundestages, Privatisierung im Strafvollzug, 2007, abrufbar unter https://www.bundestag.de/resource/blob/407046/27f9d04e8dc54423e2696a2cc058251f/wd-7-076-07-pdf-data.pdf, zuletzt abgerufen am 16. 8. 2019.

Wolff, Hans J./*Bachof*, Otto/*Stober*, Rolf/*Kluth*, Winfried: Verwaltungsrecht II, 7. Aufl., München 2010.

Wolff, Heinrich Amadeus/*Brink*, Stefan (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 28. Edition, München 2019.

Wollenschläger, Ferdinand: Staatliche Verbraucherinformation als neues Instrument des Verbraucherschutzes, Möglichkeiten und Grenzen der Informationsbefugnis nach dem Verbraucherinformationsgesetz am Beispiel der Pankower Ekelliste und das Problem staatlicher Marktinformation, in: VerwArch 102 (2011), S. 20 – 50.

Wulffen, Matthias von/*Schütze*, Bernd: SGB X – Sozialverwaltungsverfahren und Sozialdatenschutz, Kommentar, 8. Aufl., München 2014.

Zimmerlich, Antje: Der Fall Microsoft, Herausforderungen für das Wettbewerbsrecht durch die Internetökonomie, in: WRP 2004, S. 1260 – 1272.

Zimmerlich, Antje: Marktmacht in dynamischen Märkten, Die Abgrenzung des sachlich relevanten Marktes in Märkten der Internetökonomie, Frankfurt/Main 2011.

Zundel, Frank P.: Outsourcing in der öffentlichen Verwaltung, in: CR 2003, S. 763 – 768.

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/

Sachwortverzeichnis

DOI https://doi.org/10.3790/978-3-428-55931-2 | Generated on 2025-12-21 03:42:30
OPEN ACCESS | Licensed under CC BY-NC-ND 4.0 | https://creativecommons.org/about/cclicenses/